No. 17-961

IN THE
Supreme Court of the United States

THEODORE H. FRANK, ET AL.,
Petitioners,

v.

PALOMA GAOS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL.,
Respondents.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF FOR CLASS RESPONDENTS

KASSRA P. NASSIRI
Counsel of Record
NASSIRI & JUNG LLP
47 Kearny St.
Suite 700
San Francisco, CA 94108
(415) 762-3100
kass@njfirm.com

JEFFREY A. LAMKEN
MICHAEL G. PATTILLO, JR.
JAMES A. BARTA
WILLIAM J. COOPER
MOLOLAMKEN LLP
The Watergate, Suite 660
600 New Hampshire Ave., N.W.
Washington, D.C. 20037
(202) 556-2000
jlamken@mololamken.com

Counsel for Class Respondents

(Additional Counsel Listed on Inside Cover)

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

MICHAEL ASCHENBRENER
KAMBERLAW, LLC
201 Milwaukee St.
Suite 200
Denver, CO 80206
(303) 222-0281
masch@kamberlaw.com

JUSTIN B. WEINER
JORDAN A. RICE
MOLOLAMKEN LLP
300 N. LaSalle St.
Chicago, IL 60654
(312) 450-6700

QUESTION PRESENTED

Federal Rule of Civil Procedure 23(b)(3) permits representatives to maintain a class action where so doing "is superior to other available methods for fairly and efficiently adjudicating the controversy," and Rule 23(e)(2) requires that a settlement that binds class members must be "fair, reasonable, and adequate." The question presented is:

Whether, or in what circumstances, a class-action settlement that provides a *cy pres* award of class-action proceeds but no direct relief to class members comports with the requirement that a settlement binding class members must be "fair, reasonable, and adequate" and supports class certification.

TABLE OF CONTENTS

	Page
Introduction	1
Statement	3
I. Legal Framework	3
A. The Federal Rules Process	3
B. Rule 23's Requirements for Class Actions	4
C. Rule 23's Protections Governing Settlements	5
D. Congressional Revisions to Class-Action Procedures	6
E. Judicial and Congressional Consideration of *Cy Pres* Settlements	7
II. Proceedings Below	11
A. Proceedings Before the District Court	11
1. The Complaints and Resulting Motions	11
2. Uncertainty and Mediation Drive the Parties to Settlement	12
3. The Selection of *Cy Pres* Recipients	14
4. District Court Approval	16
B. Proceedings in the Court of Appeals	18
Summary of Argument	20
Argument	23
I. The Federal Rules and Relevant Statutes Do Not Prohibit *Cy Pres* Settlements	25

TABLE OF CONTENTS—Continued

Page

A. The Text, Structure, and History of Rule 23 Do Not Support Petitioners' Prohibition on *Cy Pres* Settlements 25

1. Petitioners' Categorical Ban Defies Rule 23(e)'s Clear Text 25

2. Petitioners' Categorical Ban Ignores Rule 23(e)'s Structure and History 28

B. Federal Courts Have Identified the Limited Contexts Where *Cy Pres* Settlements Might Satisfy Rule 23(e) 31

C. Rule 23(b)(3)'s "Superiority" Requirement Does Not Preclude *Cy Pres* Resolution 35

D. Petitioners' and Their *Amici*'s Remaining Arguments Fail 37

1. Petitioners' First Amendment Argument Is Waived and Meritless 37

2. *Cy Pres* Raises Neither Redressability Nor Rules Enabling Act Concerns 38

II. Petitioners' Proposed Attorney's Fees Rules Are Misplaced and Unfounded 40

A. Petitioners' Attorney's Fees Proposals Are Not Properly Before the Court 40

B. Petitioners' Fee Rules Defy Text and History 41

TABLE OF CONTENTS—Continued

	Page
III. Petitioners' Policy Arguments Fail	43
A. Existing Standards Address Petitioners' Concerns	43
B. Petitioners' Accusations Are Unfounded	47
IV. This Settlement Complies with Rule 23	48
A. The Settlement Provides Valuable Prospective Relief To Prevent Violations	48
B. The District Court Properly Found the Cash Component Adequate and Non-Distributable	49
C. The District Court Did Not Abuse Its Discretion in Approving Recipients	52
V. The Government's Jurisdictional Argument Counsels Dismissing the Petition as Improvidently Granted	54
Conclusion	56
Appendix A – Federal Rule of Civil Procedure 23	1a
Appendix B – AARP Foundation Proposal	9a
Appendix C – Berkman Center for Internet & Society at Harvard University Proposal	20a
Appendix D – Carnegie Mellon Proposal	48a
Appendix E – Center for Information, Society and Policy at IIT Chicago-Kent College of Law Proposal	86a
Appendix F – Stanford Law School's Center for Internet and Society Proposal	114a

TABLE OF CONTENTS—Continued

Page

Appendix G – World Privacy Forum Proposal 167a

TABLE OF AUTHORITIES

Page(s)

CASES

Adarand Constructors, Inc. v. *Mineta*, 534 U.S. 103 (2001) 54, 55

In re Airline Ticket Comm'n Antitrust Litig., 268 F.3d 619 (8th Cir. 2001) 44

In re Airline Ticket Comm'n Antitrust Litig., 307 F.3d 679 (8th Cir. 2002) 7

Amchem Prods., Inc. v. *Windsor*, 521 U.S. 591 (1997) ..... *passim*

Amgen Inc. v. *Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455 (2013) 3, 24, 30

Arizona v. *Hicks*, 480 U.S. 321 (1987) 56

ATD Grp. v. *Frank*, No. 16-2850, 2017 WL 4014951 (2d Cir. Mar. 29, 2017) 47

In re Baby Prods. Antitrust Litig., 708 F.3d 163 (3d Cir. 2013) ..... *passim*

In re BankAmerica Corp. Sec. Litig., 775 F.3d 1060 (8th Cir. 2015) 31

Bay Area Laundry & Dry Cleaning Pension Tr. Fund v. *Ferbar Corp. of Cal., Inc.*, 522 U.S. 192 (1997) 37

In re Bayer Corp. Litig., No. 09-md-2023, 2013 WL 12353998 (E.D.N.Y. Nov. 8, 2013) 44

Beastie Boys v. *Monster Energy Co.*, 983 F. Supp. 2d 369 (S.D.N.Y. 2014) 28

Beech Aircraft Corp. v. *Rainey*, 488 U.S. 153 (1988) 25

Boeing Co. v. *Van Gemert*, 444 U.S. 472 (1980) 41, 42

TABLE OF AUTHORITIES—Continued

Page(s)

Bowen v. *Massachusetts*, 487 U.S. 879 (1988) 39

Califano v. *Yamasaki*, 442 U.S. 682 (1979) 3, 39

Caperton v. *A. T. Massey Coal Co.*, 556 U.S. 868 (2009) 46

Carnegie v. *Household Int'l, Inc.*, 376 F.3d 656 (7th Cir. 2004) 36

Carpenter v. *United States*, 138 S. Ct. 2206 (2018) 56

In re Cendant Corp. Litig., 264 F.3d 201 (3d Cir. 2001) 6

Christian Legal Soc'y Chapter of Univ. of Cal. v. *Martinez*, 561 U.S. 661 (2010) 38

City of Los Angeles v. *Lyons*, 461 U.S. 95 (1983) 39

Connick v. *Thompson*, 563 U.S. 51 (2011) 43

In re Dry Max Pampers Litig., 724 F.3d 713 (6th Cir. 2013) 44

Eisen v. *Carlisle*, 417 U.S. 156 (1974) 37

Eubank v. *Pella Corp.*, 753 F.3d 718 (7th Cir. 2014) 5

Evans v. *Jeff D.*, 475 U.S. 717 (1986) 25

In re Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011) 12

Fischel v. *Equitable Life Assurance Soc'y of U.S.*, 307 F.3d 997 (9th Cir. 2002) 54

Fox v. *Vice*, 563 U.S. 826 (2011) 54

TABLE OF AUTHORITIES—Continued

Page(s)

Fraley v. *Facebook, Inc.*,
966 F. Supp. 2d 939 (N.D. Cal. 2013) 44

Friends of the Earth, Inc. v. *Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167 (2000) 38

Gallego v. *Northland Grp. Inc.*,
814 F.3d 123 (2d Cir. 2016) 45, 52

Gill v. *Whitford*, 138 S. Ct. 1916 (2018) 39

Glover v. *United States*, 531 U.S. 198 (2001) 37

Granite Rock Co. v. *Int'l Bhd. of Teamsters*,
561 U.S. 287 (2010) 37

Guidry v. *Sheet Metal Workers Nat'l Pension Fund*, 493 U.S. 365 (1990) 26

Hanlon v. *Chrysler Corp.*, 150 F.3d 1011
(9th Cir. 1998) 45

Holtzman v. *Turza*, 728 F.3d 682
(7th Cir. 2013) 32

Hughes v. *Kore of Ind. Enter., Inc.*,
731 F.3d 672 (7th Cir. 2013) 8, 31, 32, 33

Izumi Seimitsu Kogyo Kabushiki Kaisha v. *U.S. Philips Corp.*, 510 U.S. 27 (1993) 54

Kellogg Brown & Root Servs., Inc. v. *United States ex rel. Carter*,
135 S. Ct. 1970 (2015) 25

Klier v. *Elf Atochem N. Am., Inc.*,
658 F.3d 468 (5th Cir. 2011) ..... *passim*

Koby v. *ARS Nat'l Servs., Inc.*,
846 F.3d 1071 (9th Cir. 2017) 44

TABLE OF AUTHORITIES—Continued

Page(s)

Lane v. *Facebook*, 696 F.3d 811 (9th Cir. 2012) 9

Low v. *LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) 12

Lujan v. *Defs. of Wildlife*, 504 U.S. 555 (1992) 38

In re Lupron Mktg. & Sales Practices Litig., 677 F.3d 21 (1st Cir. 2012) 9, 31, 33, 52

Lytle v. *Household Mfg., Inc.*, 494 U.S. 545 (1990) 41

Marshall v. *Nat'l Football League*, 787 F.3d 502 (8th Cir. 2015) 39

Masters v. *Wilhelmina Model Agency, Inc.*, 473 F.3d 423 (2d Cir. 2007) 31

McDonough v. *Toys "R" Us, Inc.*, 80 F. Supp. 3d 626 (E.D. Pa. 2015) 50

In re MGM Mirage Sec. Litig., 708 F. App'x 894 (9th Cir. 2017) 33

In re Microsoft Corp. Antitrust Litig., 185 F. Supp. 2d 519 (D. Md. 2002) 45

Miller v. *Steinbach*, No. 66 Civ. 356, 1974 WL 350 (S.D.N.Y. Jan. 3, 1974) 8

In re Motor Fuel Temperature Sales Practices Litig., 872 F.3d 1094 (10th Cir. 2017) 37, 38

Nachshin v. *AOL, LLC*, 663 F.3d 1034 (9th Cir. 2011) 33, 47

TABLE OF AUTHORITIES—Continued

Page(s)

Nat'l Ass'n of Chain Drug Stores v. *New Eng. Carpenters Health Benefits Fund*, 582 F.3d 30 (1st Cir. 2005) 25

New York v. *Reebok Int'l Ltd.*, 96 F.3d 44 (2d Cir. 1996) 8, 32

Nix v. *Whiteside*, 475 U.S. 157 (1986) 43

In re Online DVD-Rental Antitrust Litig., 779 F.3d 934 (9th Cir. 2015) 50

Ortiz v. *Fibreboard Corp.*, 527 U.S. 815 (1999) 45

Pecover v. *Elec. Arts Inc.*, No. 08-cv-02820, 2013 WL 12121865 (N.D. Cal. May 30, 2013) 44

In re Pharm. Indus. Average Wholesale Price Litig., 588 F.3d 24 (1st Cir. 2009) ..... *passim*

Phillips Petrol. Corp. v. *Shutts*, 472 U.S. 797 (1985) 35, 38

Polar Int'l Brokerage Corp. v. *Reeve*, 187 F.R.D. 108 (S.D.N.Y. 1999) 44

Powell v. *Ga.-Pac. Corp.*, 119 F.3d 703 (8th Cir. 1997) 8, 32

In re Prudential Ins. Co. Am. Sales Practice Litig., 148 F.3d 283 (3d Cir. 1998) 26, 28

Sebelius v. *Cloer*, 569 U.S. 369 (2013) 44

Six (6) Mexican Workers v. *Ariz. Citrus Growers*, 904 F.2d 1301 (9th Cir. 1990) ..... *passim*

Spokeo, Inc. v. *Robins*, 136 S. Ct. 1540 (2016) 54, 55, 56

TABLE OF AUTHORITIES—Continued

Page(s)

Steel Co. v. *Citizens for a Better Env't*, 523 U.S. 83 (1998) 38

In re Subway Footlong Mktg. Litig., 869 F.3d 551 (7th Cir. 2017) 44

Sullivan v. *DB Invs., Inc.*, 667 F.3d 273 (3d Cir. 2011) 39

Synfuel Techs., Inc. v. *DHL Express (USA), Inc.*, 463 F.3d 646 (7th Cir. 2006) 26

Taylor v. *Freeland & Kronz*, 503 U.S. 638 (1992) 41

Tex. Dep't of Hous. & Cmty. Affairs v. *Inclusive Cmtys. Project, Inc.*, 135 S. Ct. 2507 (2015) 50

Time, Inc. v. *Hill*, 385 U.S. 374 (1967) 56

United States v. *Johnston*, 268 U.S. 220 (1925) 53

United States v. *Paramount Pictures, Inc.*, 334 U.S. 131 (1948) 52

United States v. *Sanchez-Gomez*, 138 S. Ct. 1532 (2018) 38

In re Wells Fargo Sec. Litig., 991 F. Supp. 1193 (N.D. Cal. 1998) 51

Wyeth v. *Levine*, 555 U.S. 555 (2009) 30

In re Zynga Privacy Litig., No. C 10-04680, 2011 WL 7479170 (N.D. Cal. June 15, 2011) 12

In re Zynga Privacy Litig., 750 F.3d 1098 (9th Cir. 2014) 13, 17

TABLE OF AUTHORITIES—Continued

Page(s)

CONSTITUTIONAL PROVISIONS, STATUTES, AND RULES

U.S. Const. art. III 22, 38, 39, 55
U.S. Const. amend. I 22, 37, 38, 55
U.S. Const. amend. IV 56
Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 ..... *passim*
28 U.S.C. § 1712(a) 7, 29, 42
28 U.S.C. § 1712(e) 29
28 U.S.C. § 1715(a) 6, 30
28 U.S.C. § 1715(b) 6, 30
28 U.S.C. § 1715(d) 6, 30
Private Securities Litigation Reform Act of 1995, Pub. L. No. 104-67, 109 Stat. 737 ..... 6, 42
15 U.S.C. § 77z-1(a)(6) 6, 42
Stored Communications Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 ..... *passim*
18 U.S.C. § 2702(a)(1) 12, 56
18 U.S.C. § 2702(a)(2) 56
18 U.S.C. § 2702(b)(3) 12, 48
18 U.S.C. § 2702(c) 13
15 U.S.C. § 1692k(a)(3) 27
28 U.S.C. § 455 47
28 U.S.C. § 2072(b) 39
28 U.S.C. § 2074(a) 4
Fed. R. Civ. P. 11 27
Fed. R. Civ. P. 23 ..... *passim*

TABLE OF AUTHORITIES—Continued

Page(s)

Fed. R. Civ. P. 23(a) 4, 16
Fed. R. Civ. P. 23(a)(4) 45
Fed. R. Civ. P. 23(b) 17, 40
Fed. R. Civ. P. 23(b)(3) ..... *passim*
Fed. R. Civ. P. 23(e) ..... *passim*
Fed. R. Civ. P. 23(e)(1) 5
Fed. R. Civ. P. 23(e)(2) ..... *passim*
Fed. R. Civ. P. 23(e)(2)(C)(iii) 42
Fed. R. Civ. P. 23(e)(4) 5
Fed. R. Civ. P. 23(e)(5) 5
Fed. R. Civ. P. 23(g)(4) 5
Fed. R. Civ. P. 23(h) ..... *passim*
Fed. R. Civ. P. 23(h)(1) 5
Fed. R. Civ. P. 23(h)(2) 5
Fed. R. Civ. P. 23(h)(3) 5

LEGISLATIVE MATERIALS

Fairness in Class Action Litigation and Furthering Asbestos Claim Transparency Act of 2017, H.R. 985, 115th Cong. 10, 30
Stop Settlement Slush Funds Act of 2017, H.R. 732, 115th Cong. 10
H.R. Rep. No. 115-72 (2017) 10, 11
S. Rep. No. 109-14 (2005) 10, 29
151 Cong. Rec. S1,007 (daily ed. Feb. 7, 2005) 29

TABLE OF AUTHORITIES—Continued

Page(s)

Class Action Fairness Act of 1999: Hearing on S. 353 Before the Subcomm. on Admin. Oversight & the Courts of the S. Comm. on the Judiciary, 106th Cong. (1999) 10

Class Action Fairness Act of 2003: Hearing on H.R. 1115 Before the H. Comm. on the Judiciary, 108th Cong. (2003) 7, 10, 29

Class Actions Seven Years After the Class Action Fairness Act: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 112th Cong. (2012) 10, 29

Consumers Shortchanged? Oversight of the Justice Department's Mortgage Lending Settlements: Hearing Before the Subcomm. on Regulatory Reform, Commercial & Antitrust Law of the H. Comm. on the Judiciary, 114th Cong. (2015)..... 30

Examination of Litigation Abuses: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 113th Cong. (2013)..... 29

State of Class Actions Ten Years After the Enactment of the Class Action Fairness Act: Hearing Before the H. Subcomm. on the Constitution & Civil Justice of the H. Comm. on the Judiciary, 114th Cong. (2015) 29

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES

Am. Law. Inst., *Principles of the Law, Aggregate Litigation* (2010) ..... *passim*

R. Bone, *Justifying Class Action Limits: Parsing the Debates over Ascertainability and Cy Pres*, 65 U. Kan. L. Rev. 913 (2017) 46

D. Dobbs, *Law of Remedies* (2d ed. 1993) 56

Fed. Jud. Ctr., *Manual for Complex Litigation* (4th) (2004) 34

Fed. R. Civ. P. 23 advisory committee's note to 2003 amendment 27, 25, 41, 45

Fed. R. Civ. P. 23 advisory committee's note to 2018 amendment 42

B. Fitzpatrick, *An Empirical Study of Class Action Settlements and Their Fee Awards*, 7 J. Empirical Legal Stud. 811 (2010) 9

W. Page Keeton et al., *Prosser and Keeton on Torts* (5th ed. 1984) 56

Minutes, Meeting of the Advisory Committee on Civil Rules (Apr. 23-24, 2001) 26

R. Mulheron, *The Modern Cy-près Doctrine: Applications & Implications* (2006) 7

TABLE OF AUTHORITIES—Continued

Page(s)

M. Redish, *Cy Pres Relief and the Pathologies of the Modern Class Action: A Normative and Empirical Analysis*, 62 Fla. L. Rev. 617 (2010) 9

Report by the Committee on Rules of Practice and Procedure (2016) 11, 30, 31

Restatement (Second) of Contracts (1981) 28

Restatement (Third) of Trusts (2003) 7

W. Rubenstein, *Newberg on Class Actions* (5th ed.) ..... *passim*

S. Shepherd, *Damage Distribution in Class Actions: The Cy Pres Remedy*, 39 U. Chi. L. Rev. 448 (1972) 8

C. Wright & A. Miller, *Federal Practice and Procedure* (3d ed.) 3, 4, 41, 54

IN THE

Supreme Court of the United States

NO. 17-961

THEODORE H. FRANK, ET AL.,

Petitioners,

v.

PALOMA GAOS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL.,

Respondents.

On Writ of Certiorari
to the United States Court of Appeals
for the Ninth Circuit

BRIEF FOR CLASS RESPONDENTS

INTRODUCTION

This case concerns the circumstances in which Fed. R. Civ. P. 23(e) permits settlement proceeds to be distributed to third parties to perform work that benefits class members. Such distributions are referred to as "*cy pres*" distributions because they resemble the equitable doctrine that allows funds in trust to be put to their next-best use when the original purpose becomes infeasible. In the class-action context, *cy pres* distributions are rare. They are permitted only where payment of the funds to class members is infeasible.

Petitioners propose a judicial ban on such distributions or, alternatively, specific rules governing attorney's fees (rules Congress imposed in other contexts but declined to impose here). Petitioners, however, find no support in the text, structure, or history of Rule 23 or any relevant law. Petitioners instead offer a dissertation—largely based on dubious anecdotes—assailing class actions generally. Their arguments reduce to accusations that the bar will engage in "self-deal[ing]," "subterfuge," "gamesmanship," and "gimmicks" that "sell their putative clients down the river." And they accuse the district courts charged with implementing Rule 23 of "ignoring and resisting circuit court" precedent to "permit class counsel to use class settlements to self-deal freely." Petitioners resort to attacking the bar and bench because every traditional rule of construction forecloses their proposals. And the accusations have no relevance to *this* case or *this* settlement. Petitioners ignore or mischaracterize the prospective relief the settlement provides, which brings genuine change for class members. And they ignore the carefully delineated uses to which the *cy pres* recipients will put the monetary fund, which likewise benefit class members.

Rule 23(e) permits class-action settlements where the terms are "fair, reasonable, and adequate." Outside the class-action context, parties can agree to settlements that do not provide direct monetary compensation, opting instead for injunctive relief and payments to third parties for the plaintiff's benefit. Rule 23(e) imposes no prohibition on class settlements that do the same thing. Petitioners would deem that sort of settlement unfair and unreasonable even where class members otherwise would get absolutely *nothing*. Petitioners nowhere explain why a provision requiring settlements to be fair, reasonable,

and adequate would require the less fair, less reasonable, less adequate relief of no remedy whatsoever instead.

Petitioners' brief ultimately offers a series of legislative proposals based on policy arguments. But the Federal Rules are promulgated through a rigorous process that includes consideration by the Advisory Committee, Judicial Conference approval, this Court's review, and submission to Congress. That process "limits judicial inventiveness," *Amchem Prods., Inc.* v. *Windsor*, 521 U.S. 591, 620 (1997), leaving this Court "no warrant to encumber [class-action] litigation by adopting an atextual requirement * * * that Congress, despite its extensive involvement in the * * * field, has not sanctioned." *Amgen Inc.* v. *Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 478 (2013). Petitioners seek to impose precisely such atextual requirements here.

STATEMENT

I. LEGAL FRAMEWORK

Federal Rule of Civil Procedure 23 governs the certification and administration of class actions in federal court. Rule 23 is intended to "achieve economies of time, effort, and expense, and promote uniformity of decision as to persons similarly situated" by aggregating individual claims into a single proceeding. Fed. R. Civ. P. 23 advisory committee's note to 1966 amendment; see *Califano* v. *Yamasaki*, 442 U.S. 682, 701 (1979).

A. The Federal Rules Process

The Federal Rules are promulgated only "after an extensive deliberative process involving many reviewers." *Amchem*, 521 U.S. at 620. New rules and changes to existing rules are proposed by the Advisory Committee on Civil Rules. 4 C. Wright & A. Miller, *Federal Practice and Procedure* § 1001 n.16 (3d ed.). Proposals are then

reviewed by subcommittees, circulated to the public for comment, and revised by the Advisory Committee before being submitted to the United States Judicial Conference. *Ibid.* If a proposed rule or amendment is accepted by the Judicial Conference, it is submitted to this Court. *Ibid.*

If this Court accepts the rule, it sends it to Congress for consideration. 4 Wright & Miller, *supra*, § 1001; see 28 U.S.C. § 2074(a). The rule "becomes effective" the following December "unless Congress takes action to alter or reject it." 4 Wright & Miller, *supra*, § 1001 n.16; see 28 U.S.C. § 2074(a). "The text of a rule thus proposed and reviewed" necessarily "limits judicial inventiveness. Courts are not free to amend a rule outside the process Congress ordered * * *." *Amchem*, 521 U.S. at 620.

B. Rule 23's Requirements for Class Actions

Rule 23(a) establishes four prerequisites for class actions, requiring judicial findings that:

> (1) the class is so numerous that joinder of all members is impracticable;
>
> (2) there are questions of law or fact common to the class;
>
> (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and
>
> (4) the representative parties will fairly and adequately protect the interests of the class.

Fed. R. Civ. P. 23(a).

This case involves an "opt-out" class action for damages. Such actions are appropriate where the recoveries are too small to "'provide the incentive for any individual to bring a solo action prosecuting his or her rights.'"

Amchem, 521 U.S. at 617. Rule 23(b)(3) imposes two additional prerequisites for such cases. One is "predominance": "[Q]uestions of law or fact common to class members" must "predominate over any questions affecting only individual members." Fed. R. Civ. P. 23(b)(3). The other is "superiority": A class action must be "superior to other available methods for fairly and efficiently adjudicating the controversy." *Ibid.*

C. Rule 23's Protections Governing Settlements

To assure procedural fairness for absent class members, Rule 23(e) provides that class actions may not be "settled, voluntarily dismissed, or compromised" without district-court approval. The court "must direct notice in a reasonable manner to all class members who would be bound by the proposal." Fed. R. Civ. P. 23(e)(1). "Any class member may object to the proposal," *id.* 23(e)(5), or "request exclusion" from the class and thus opt out of any final judgment, *id.* 23(e)(4). The court may approve the proposed settlement, voluntary dismissal, or compromise "only after a hearing and on finding that it is fair, reasonable, and adequate." *Id.* 23(e)(2).

Rule 23(h) provides for court oversight of attorney's fees. Class counsel's request for fees must be made by motion, and notice must be provided to the class. Fed. R. Civ. P. 23(h)(1). Class members may object. *Id.* 23(h)(2). The court may award only "reasonable attorney's fees." *Id.* 23(h). And the court "must find the facts and state its legal conclusions" supporting its decision. *Id.* 23(h)(3).

"Class counsel must fairly and adequately represent the interests of the class." Fed. R. Civ. P. 23(g)(4). Class counsel are thus required to "'act as conscientious fiduciaries.'" *Eubank* v. *Pella Corp.*, 753 F.3d 718, 724 (7th Cir. 2014). The settlement-approval standards in Rule 23(e) likewise require district courts to "act[ ] as a fiduci-

ary guarding the rights of absent class members." *In re Cendant Corp. Litig.*, 264 F.3d 201, 231 (3d Cir. 2001); see 4 W. Rubenstein, *Newberg on Class Actions* §13:40 n.4 (5th ed.) (collecting cases). "When reviewing settlements" under Rule 23(e), moreover, district courts "must ensure class counsel have met their ongoing duty" to class members. *In re Pharm. Indus. Average Wholesale Price Litig.*, 588 F.3d 24, 36 n.12 (1st Cir. 2009).

D. Congressional Revisions to Class-Action Procedures

Congress has repeatedly revisited the rules governing class actions.

In 1995, Congress enacted the Private Securities Litigation Reform Act ("PSLRA"), Pub. L. No. 104-67, 109 Stat. 737, to address securities-litigation class actions and related issues. Among other things, the Act limited the attorney's fees that can be "awarded by the court to counsel for the plaintiff class" in securities-fraud cases to "a reasonable percentage of the amount of any damages and prejudgment interest *actually paid to the class.*" 15 U.S.C. §77z-1(a)(6) (emphasis added).

A decade later, Congress passed the Class Action Fairness Act of 2005 ("CAFA"), Pub. L. No. 109-2, 119 Stat. 4. Among other things, CAFA created a role for Executive Branch and state officials in ensuring the fairness of class actions: It provides that the Attorney General of the United States, and the attorney general or appropriate official in each State, must be given notice of class-action settlements. 28 U.S.C. §1715(a), (b). The district court cannot approve a settlement until those officials have had 90 days to review it. *Id.* §1715(d). Federal and state governments can, and sometimes do, file statements of interest in response to such notices. U.S. Br. 1-2.

CAFA also created rules governing attorney's fees for "coupon settlements," in which defendants provide coupons for their goods or services to class members in exchange for a release from liability. CAFA provides that "any attorney's fee award to class counsel that is attributable to [an] award of coupons shall be based on the value to class members of the coupons *that are redeemed*." 28 U.S.C. § 1712(a) (emphasis added). Congress had considered but declined to enact broader limits. See, *e.g.*, *Class Action Fairness Act of 2003: Hearing on H.R. 1115 Before the H. Comm. on the Judiciary*, 108th Cong. 111-112 (2003) (discussing fee awards as "a percentage of the fund *actually disbursed* to class members").

E. Judicial and Congressional Consideration of *Cy Pres* Settlements

1. This case concerns a "*cy pres*" distribution. The term *cy pres*—short for *cy pres comme possible*, or "as near as possible"—entered the law as a trusts-and-estates doctrine. R. Mulheron, *The Modern Cy-près Doctrine: Applications & Implications* 2-3 (2006). In that context, *cy pres* can "save testamentary charitable gifts that would otherwise fail" by choosing "an alternate recipient that will best serve the gift's original purpose." *In re Airline Ticket Comm'n Antitrust Litig.*, 307 F.3d 679, 682 (8th Cir. 2002). The doctrine applies where fulfilling the testator's original directive "becomes unlawful, impossible, impracticable * * *, or * * * wasteful." *Restatement (Third) of Trusts* § 67 (2003).

Similar equitable principles have been invoked in class-action litigation. For example, when a class action results in a monetary payment, the parties may agree that, if some amount goes unclaimed after the claims process, the remainder shall go to "a charity working on

issues related to the group's underlying causes of action." 4 *Newberg*, *supra*, § 12:32.

In unusual circumstances, "the class members are so numerous and the individual claims so small that individualized distributions are, as a practical matter, impossible." 4 *Newberg*, *supra*, § 12:26. Where that occurs, the parties may agree, and a court may find, that "*all* of the class action recovery (net of fees and expenses)" should be "directed to a charity whose mission is consistent with the causes of action in the litigation." *Ibid.* Such distributions can provide non-monetary or indirect benefits to the class, while avoiding "the effective exclusion of a substantial number of small claimants from the benefits of any class action, the dilution of the deterrent effect of a recovery on behalf of the class, and the unjust enrichment of the defendant." S. Shepherd, *Damage Distribution in Class Actions: The Cy Pres Remedy*, 39 U. Chi. L. Rev. 448, 448 (1972); see 4 *Newberg*, *supra*, § 12:26 (listing "deterrence," "indirect compensation to the plaintiff class," and "finality and repose to defendant" as relevant goals).

Such settlements were approved shortly after the modernization of Rule 23 in 1966, see, *e.g.*, *Miller* v. *Steinbach*, No. 66 Civ. 356, 1974 WL 350 (S.D.N.Y. Jan. 3, 1974), and—in the ensuing half century—have been upheld or endorsed by seven federal courts of appeals where distribution to class members proves infeasible.[1]

---

[1] See *Pharm. Indus.*, 588 F.3d at 35 (1st Cir.); *New York* v. *Reebok Int'l Ltd.*, 96 F.3d 44, 49 (2d Cir. 1996); *In re Baby Prods. Antitrust Litig.*, 708 F.3d 163, 172-174 (3d Cir. 2013); *Klier* v. *Elf Atochem N. Am., Inc.*, 658 F.3d 468, 475 (5th Cir. 2011); *Hughes* v. *Kore of Ind. Enter., Inc.*, 731 F.3d 672, 675 (7th Cir. 2013); *Powell* v. *Ga.-Pac. Corp.*, 119 F.3d 703, 706-707 (8th Cir. 1997); *Lane* v. *Facebook*, 696 F.3d 811, 819 (9th Cir. 2012).

But *cy pres* settlements remain rare. Between 1974 and 1990, fewer than one class action per year ended with a *cy pres* distribution. M. Redish, *Cy Pres Relief and the Pathologies of the Modern Class Action: A Normative and Empirical Analysis*, 62 Fla. L. Rev. 617, 653 (2010). From 1990 to 2008, a tiny portion of the class actions that settled each year—an average of 5—resulted in *cy pres* settlements. *Id.* at 653, 658 (identifying 86 *cy pres* settlements over an 18-year period, including some where damages were paid directly to class members); see B. Fitzpatrick, *An Empirical Study of Class Action Settlements and Their Fee Awards*, 7 J. Empirical Legal Stud. 811, 817-818 (2010) (340 class-action settlements per year in 2006-2007).

2. The courts of appeals have converged on the circumstances where *cy pres* distribution may meet Rule 23's "fair, reasonable, and adequate" standard. *First*, direct distribution of the funds to class members must be infeasible. Am. Law. Inst., *Principles of the Law, Aggregate Litigation* §3.07(c) (2010) ("ALI Principles"); *Klier*, 658 F.3d at 475. *Second*, the recipient of the funds must have a mission tied to rectifying problems similar to those underlying the case. ALI Principles §3.07(c); *In re Lupron Mktg. & Sales Practices Litig.*, 677 F.3d 21, 33 (1st Cir. 2012). That requirement ensures that, even if class members do not receive direct cash payment, they benefit from the distribution. The American Law Institute has identified a third requirement: The "court or any party" must not have "any significant prior affiliation with the intended recipient that would raise substantial questions about whether the selection of the recipient was made on the merits." ALI Principles §3.07 cmt. b.

3. Although Congress has repeatedly considered *cy pres* settlements, it has declined to overturn governing

standards. When Congress was deliberating over CAFA, the RAND Institute submitted a report addressing *cy pres* distributions. *Class Action Fairness Act of 2003: Hearing on H.R. 1115 Before the H. Comm. on the Judiciary*, 108th Cong. 111-112 (2003). *Cy pres* was mentioned throughout the legislative process. See, *e.g.*, S. Rep. No. 109-14, at 17, 19 (2005); *Class Action Fairness Act of 1999: Hearing on S. 353 Before the Subcomm. on Admin. Oversight & the Courts of the S. Comm. on the Judiciary*, 106th Cong. 53 (1999) (John P. Frank). Congress provided special rules for "coupon" settlements, see p. 7, *supra*, but not *cy pres*.

Congress has returned to *cy pres* settlements since. See, *e.g.*, *Class Actions Seven Years After the Class Action Fairness Act: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 112th Cong. 2, 40, 96 (2012). Legislation addressing fees from *cy pres* settlements has passed one chamber of Congress and is pending in the other. See Fairness in Class Action Litigation and Furthering Asbestos Claim Transparency Act of 2017, H.R. 985, 115th Cong. §1718. So too is legislation addressing the Justice Department's ability to enter into such settlements. See Stop Settlement Slush Funds Act of 2017, H.R. 732, 115th Cong. §2; H.R. Rep. No. 115-72, at 12-13 (2017). But Congress has not enacted those bills to date.

The Rules Advisory Committee has considered the issue, but found no reason to alter existing rules. One subcommittee developed "a possible rule amendment and a possible Committee Note" that drew "very considerable attention." *Report by the Committee on Rules of Practice and Procedure* 213 (2016). But it recommended against pursuing the amendment, noting that the circuits were converging around the ALI Principles, that some

commenters had raised Rules Enabling Act concerns, and that it would be challenging to "develop[ ] specifics for a rule provision." *Id.* at 213-214. "The Committee accepted this recommendation." *Id.* at 424.

II. Proceedings Below

A. Proceedings Before the District Court

This case arises from a previously little-known aspect of Google's web-search product. When users enter a query in Google Search, Google displays the results on a page headed with a Uniform Resource Locator ("URL") that includes the search terms. Pet. App. 4. For example, a search for "depression and medical leave" would return a page with a URL similar to "http://www.google.com/search?q=depression+and+medical+leave." See Pet. App. 4 & n.1. Web browsers report to websites the URL of the page containing the link that was clicked to reach their website—*i.e.*, the page that "referred" them. Pet. App. 4. Users' search terms thus are sent to third-party websites in the form of these "referrer headers." *Ibid.* "This information is then disseminated further, since several web analytics services" also "collect the search query from the referrer header." Pet. App. 32-33.

1. *The Complaints and Resulting Motions*

Alarmed by that privacy invasion, Paloma Gaos filed suit against Google in the Northern District of California in October 2010. The complaint alleged that Google's disclosure of her searches in "referrer headers" violated the Stored Communications Act ("SCA"), 18 U.S.C. §§2701 *et seq.* D. Ct. Doc. 1 ¶¶86-97. The SCA prohibits a provider of a "remote computing service" from "knowingly divulg[ing] * * * the contents of a communication while in electronic storage by that service," without the "lawful consent" of the communication's originator. 18 U.S.C. §2702(a)(1), (b)(3). Gaos also alleged violations of various

California laws. D.Ct. Doc. 1 ¶¶98-137. Filed on behalf of a putative class comprising all U.S. persons who submitted Google search queries after October 25, 2006, *id.* ¶74, the complaint sought "injunctive and other equitable relief as is necessary to protect the interests of Plaintiff [and] the Class," as well as actual and statutory damages, *id.* at 34.

Google moved to dismiss, urging that Gaos lacked standing. D.Ct. Doc. 19. In April 2011, the district court granted the motion. J.A. 16-22. Gaos filed an amended complaint that again alleged SCA violations, but replaced the state-law statutory claims with common-law claims. J.A. 23-25. In March 2012, the court granted Google's motion to dismiss Gaos's state-law claims, but denied the motion as to the SCA claim. J.A. 23-31.

In May 2012, Gaos filed a second amended complaint, adding another class representative and additional state-law claims. J.A. 84; C.A.S.E.R. 781-786. Google again moved to dismiss. D.Ct. Doc. 44; Pet. App. 70.

2. *Uncertainty and Mediation Drive the Parties to Settlement*

While the parties litigated, the U.S. District Court for the Northern District of California dismissed three other cases that likewise alleged SCA violations based on disclosure of referrer headers. See *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011); *In re Zynga Privacy Litig.*, No. C 10-04680, 2011 WL 7479170 (N.D. Cal. June 15, 2011); *Low* v. *LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1023-1024 (N.D. Cal. 2012). While this case was pending, the Ninth Circuit affirmed the dismissal in *In re Zynga Privacy Litigation*, 750 F.3d 1098 (9th Cir. 2014).

Given the resulting uncertainty, counsel repeatedly met to discuss settlement. C.A.S.E.R. 61 ¶¶6-9 & 83 ¶6.

While the case was not going well for Gaos, Google confronted potentially staggering liability if she prevailed.[2] In 2013, the parties negotiated before an experienced class-action mediator, who made a proposal that became the framework for a settlement. C.A.S.E.R. 62 ¶¶11-12, 83-84 ¶¶8-9. The parties negotiated the details over two months. C.A.S.E.R. 62 ¶¶13-17, 84 ¶¶9-10. Throughout, class counsel insisted on "prospective relief designed to notify users as to Google's conduct so that users can make informed choices about whether and how to use Google search." C.A.S.E.R. 62 ¶18; see C.A.S.E.R. 84 ¶11, 132 ¶23.

Permanent prospective relief. Under the final settlement, Google was obligated to make new disclosures on three of its web pages—a general FAQs page, a Privacy FAQs for Google Web History page, and a Key Terms page—concerning its handling of search-query data. Pet. App. 82; see Pet. App. 73 (defining the agreed-upon disclosures). The SCA requires "consent" before certain information can be shared. P. 11, *supra*. As the district court explained, the changes to Google's disclosures "advise search users of [Google's] conduct and policies so that users can make an informed choice about whether and how to use Defendant's search engine." J.A. 92. Those disclosures now explain how search queries are disclosed to third-party websites. Pet. App. 109-111. While petitioners state that Google retained previously made changes, Pet. Br. 9, that is incorrect: As explained below (pp. 48-49, *infra*), the settlement required new and additional disclosures.

---

[2] Because the potential class exceeded 100 million, Pet. App. 52, statutory damages of $1,000 per violation under the SCA, 18 U.S.C. §2702(c), could exceed $100 billion.

Monetary payments. The settlement also provided that Google would pay $8.5 million. The district court recognized that, "because of the size of the class"—estimated at over 100 million persons—"actual remuneration * * * to an individual class member is virtually impossible. * * * The cost of administration of that would dwarf any possible settlement." J.A. 33.

The parties therefore agreed that, after payment of fees and costs, the remaining funds would be distributed to third parties that would use the money "to promote public awareness and education, and/or to support research, development, and initiatives, related to protecting privacy on the Internet." Pet. App. 82-84. The "more robust" disclosures required, and "the cy pres efforts," were to "mak[e] sure that people are informed and give informed consent" concerning disclosure of their referrer headers. J.A. 38.

3. *The Selection of* Cy Pres *Recipients*

Class counsel sought *cy pres* recipients that (1) lacked conflicts of interest; (2) had track records on privacy issues; (3) targeted internet users nationwide; and (4) would use the funds to educate class members about the risks of sharing personal information with internet service providers, inform policymakers, and develop tools to address exploitation of personal data. C.A.S.E.R. 387 ¶21(a)-(c), (e). Candidates would submit detailed proposals. C.A.S.E.R. 387 ¶21(d). The parties narrowed the pool from over 20 to 7. C.A.S.E.R. 385 ¶¶14-15.

Six submitted detailed proposals to address internet privacy and the risks of involuntary information sharing. C.A.S.E.R. 387 ¶22; J.A. 53-81.[3]

- Carnegie Mellon University proposed developing new technologies to address online privacy threats, as well as computerized mechanisms to enforce the privacy policies of companies such as Google. J.A. 53-57 (App., *infra*, 48a-85a).
- The Stanford Law School Center for Internet and Society proposed "educat[ing] users" about "how to make effective online choices for privacy" and "how third party tracking and advertising practices work." J.A. 58-61 (App., *infra*, 114a-166a).
- The World Privacy Forum detailed a consumer-education campaign about privacy risks posed by online search boxes and referrer headers. J.A. 62-67 (App., *infra*, 167a-223a).

The other proposals similarly addressed online privacy risks. See, *e.g.*, J.A. 72-77 (App., *infra*, 86a-113a) (Center for Information, Society and Policy at IIT Chicago-Kent College of Law initiative to assist users in implementing privacy protections); J.A. 68-71 (App., *infra*, 9a-19a) (AARP anti-online fraud initiative); J.A. 78-81 (App., *infra*, 20a-47a) (Berkman Center for Internet and Society at Harvard University proposals for safeguarding internet privacy through policy reform, technological innovation, and consumer outreach). The court "carefully reviewed" those proposals. Pet. App. 48; see D. Ct. Doc. 65 at 6.

---

[3] The Joint Appendix includes executive summaries of each. J.A. 53-81. For the Court's convenience, the full text of each proposal is attached as an Appendix to this brief. App., *infra*, 9a-223a.

4. *District Court Approval*

The district court preliminarily approved the settlement and certified a settlement-only class in March 2014, finding the requirements of Rule 23(a) and (b)(3) satisfied. J.A. 82-100. Class resolution, it found, was superior to other methods of adjudicating the controversy: The alternatives were "either millions of separate, individual proceedings * * * or an abandonment of claims by most class members." J.A. 90. The court preliminarily found the settlement fair, reasonable, and adequate under Rule 23(e)(2). J.A. 91-97. Distributing settlement funds to class members, the court found, was infeasible: The costs of verifying and distributing payments "would exceed the total monetary benefit obtained by the class." J.A. 95-96. The proposed uses of the fund "account[ed] for the nature of this suit, m[et] the objectives of the SCA claim, and further[ed] the interests of class members." J.A. 96-97.

Four class members, including the petitioners here, objected. Pet. App. 34. Petitioners conceded the settlement amount was adequate, suggesting "[m]aybe * * * Google is overpaying." J.A. 118. But they objected to the third-party distributions on fairness and superiority grounds; they further argued that three proposed recipients were improper because class counsel had attended law schools associated with some of them, and Google had donated previously to others. Pet. App. 125-134. Petitioners also objected to the attorney's fees request, urging the court to "reduce the fee award to no more than 10% of the $8.5 million *cy pres* fund." Pet. App. 134-139; see J.A. 114-121, 164-165.

At the fairness hearing, the district court focused on the feasibility of distributing settlement funds to class members. J.A. 115-116. It explored "the benefit * * * for

the class" from the settlement, as well as whether they could receive "some direct" monetary benefit. J.A. 122-123. The comparative sizes of the class and the fund, the court recognized, posed serious "challenge[s]." J.A. 119-120.

Responding to petitioners' concerns about connections between counsel and *cy pres* recipients, Pet. App. 126-128, both lead attorneys for the class explained they had no affiliation with the recipients housed at their alma maters, J.A. 107-110. As one put it: "[T]o clarify on the record, I don't have any affiliation and I have never had any affiliation with [the] Berkman Center or with Harvard since leaving. I simply got my law degree there, and that's simply the end of it." J.A. 136; see J.A. 134 (similar). The court "appreciate[d]" that, contrary to petitioners' argument, the *cy pres* distribution was not simply an "accounting change" for Google about donations it would have made regardless. J.A. 135. The court nonetheless "ha[d] real concerns" that required "additional thought." J.A. 166. The court was leaning toward denying approval, but noted that the oral arguments had been "helpful." *Ibid.*

Ultimately, the court approved the settlement. Pet. App. 31-61. It again found class certification appropriate under Rule 23(b). Pet. App. 35-38. The court applied heightened scrutiny because settlement preceded class certification. Pet. App. 42. But it found the settlement fair, reasonable, and adequate under Rule 23(e)(2). Pet. App. 39-52. During litigation, "the Ninth Circuit's decision in *Zynga Privacy Litigation*" and other decisions created "significant and potentially case-ending weakness." Pet. App. 58-59. Absent settlement, there "was little guarantee of any benefit to the class." Pet. App. 44. The prospective relief requiring new dis-

closures was fair. Pet. App. 49-50. And the monetary fund "compare[d] favorably to" settlements in similar cases. Pet. App. 45-46.

The court found *cy pres* distribution appropriate because the fund could not be distributed to class members: With over 100 million estimated class members, "requiring proofs of claim * * * would undeniably impose a significant burden to distribute, review and then verify," and "the cost of sending out very small payments to millions of class members would exceed the total monetary benefit obtained by the class." Pet. App. 47. "Having carefully reviewed the[ir] proposals," the court found the *cy pres* recipients would "meet[ ] the objectives of the SCA, and further[ ] the interests of class members." Pet. App. 47-49. The court saw "no indication that counsel's allegiance to a particular alma mater factored into the selection process." Pet. App. 59.

The court approved attorney's fees of $2.125 million and incentive awards of $5000 for each class representative. Pet. App. 55-58. The settlement was not "easily secured" and came only after class counsel defended against "three motions to dismiss" and "extensive in-person negotiations." Pet. App. 54-55. Counsel's hours and rates "confirm[ed] the reasonableness of the percentage-based calculation." Pet. App. 56-57.

B. Proceedings in the Court of Appeals

The court of appeals affirmed. Pet. App. 1-23. It acknowledged that *cy pres* distributions are "the exception, not the rule." Pet. App. 8. But it found the district court did not clearly err or abuse its discretion in finding "the cost of verifying and 'sending out very small payments to millions of class members would exceed the total monetary benefit obtained by the class.'" Pet. App. 8-9. The court of appeals rejected petitioners' arguments that the

district court was required to use a lottery system or claims-made process. Pet. App. 9-10. The court rejected petitioners' view that, if cash distributions to class members were infeasible, a class action could not be superior to other methods of adjudicating the controversy for purposes of Rule 23(b)(3). Pet. App. 10-11.

The court of appeals found no abuse of discretion in the district court's approval of *cy pres* recipients. Pet. App. 11-21. The district court properly found that the recipients were "established" and "independent," with "nationwide reach and 'a record of promoting privacy protection on the Internet.'" Pet. App. 12. Their "detailed proposal[s]" ensured funds would be used to benefit the class. Pet. App. 5, 12-13.

The court of appeals addressed whether "'any party has any significant prior affiliation with the intended recipient that would raise substantial questions about whether the selection of the recipient was made on the merits.'" Pet. App. 14 (quoting ALI Principles § 3.07 cmt. b). It found that no "substantial question[ ]" was raised. *Ibid.* That Google had previously donated to some was not disqualifying. "Google has donated to hundreds of third-party organizations whose work implicates technology and Internet policy issues," and "some of the recipient organizations have challenged Google's Internet privacy policies in the past." Pet. App. 16 & n.6. Barring any organization that received a past donation would have prioritized "less relevant or less qualified" organizations over "the interests of the class." Pet. App. 18. Moreover, the proposed recipients had "disclos[ed] donations received from Google" and "explain[ed] how the *cy pres* funds were distinct from Google's general donations." Pet. App. 17.

The court likewise found no abuse of discretion stemming from the fact that three recipients are housed at schools class counsel attended. Pet. App. 18-21. The district court analyzed "the nature of the relationship, the timing and recency of the relationship, the significance of dealings between the recipient and the party or counsel, the circumstances of the selection process, and the merits of the recipient." Pet. App. 14, 18-21. Each school "graduates thousands of students each year," and "[a]ll class counsel swore that they have no affiliations with the specific research centers." Pet. App. 19.

Finally, the court of appeals found no abuse of discretion in the attorney's fee award. Pet. App. 21-23. The award was "commensurate with the risk posed by the action and the time and skill required to secure a successful result for the class, given that class counsel faced three motions to dismiss" and conducted extensive settlement negotiations. Pet. App. 22.

Judge Wallace dissented on one issue. He agreed that a *cy pres* distribution is "appropriate in this case." Pet. App. 23. He saw no abuse of discretion in the fee award. *Ibid.* But he would have required live testimony on whether class counsel's educational histories affected the selection of recipients. Pet. App. 23-24.

SUMMARY OF ARGUMENT

I. Petitioners' proposed categorical ban on approval of *cy pres* settlements has no support in the Federal Rules or any relevant law.

A. Under Rule 23(e), courts may approve class-action settlements that are "fair, reasonable, and adequate." That standard gives courts discretion to be exercised case-by-case in light of all relevant circumstances. Petitioners cannot explain why a *cy pres* settlement—which

provides class members indirect benefits—cannot be fair, reasonable, and adequate, when the alternative is that class members receive *no* relief. The settlement here, moreover, directly benefited class members through prospective relief.

Petitioners' proposed ban defies Rule 23's history. *Cy pres* settlements have existed for decades and have been studied by Congress and the Rules Advisory Committee. Those bodies have revised class-action standards but have declined to impose petitioners' ban. Petitioners ask this Court to circumvent the rigorous process for amending the Federal Rules.

B. The federal courts have identified limited circumstances where *cy pres* settlements may satisfy Rule 23(e). The settlement funds must be so limited, and fund-administration costs so high, that distribution to class members is infeasible. The *cy pres* recipients must serve the class-member interests pursued in the suit, so class members benefit from the funds' use. And recipients must be selected on merit, not because of affiliation with the parties. Properly applied, those established principles limit *cy pres* to situations where it is the best means of providing relief.

C. Rule 23(b)(3) does not preclude class certification where there is a *cy pres* settlement. That rule allows certification if class treatment is "superior *to other* available methods *for fairly and efficiently adjudicating the controversy*." The realistic alternative to class certification in cases with undistributably small recoveries—the only cases where *cy pres* is appropriate—is *no* suit at all. Petitioners seek to rewrite Rule 23(b)(3). The Rule asks whether class treatment is superior to "alternative" means "of adjudication"—not whether an objector would prefer no adjudication at all.

D. Petitioners' First Amendment argument was neither pressed nor passed upon below. Anyone offended by the *cy pres* recipients (or the suit itself) can opt out. The claim that *cy pres* settlements violate Article III, by failing to "redress" the plaintiffs' injuries, is misplaced. The prospective relief in the settlement here redresses class members' injuries. Redressability, moreover, concerns whether courts can provide a remedy—not whether the actual outcome is good enough. And damages in cases involving privacy injuries are *substitute* relief in any event, not a reversal of the invasion. Outside class actions, plaintiffs and defendants often agree to channel that substitute relief to third parties. Nothing prohibits class-action plaintiffs from making the same choice if Rule 23's requirements are met. For those reasons, the government's supposed Rules Enabling Act concerns lack merit. Settlements, moreover, are contracts. Judicial approval of a private agreement does not expand the court's remedial powers.

II. Petitioners' categorical rules for attorney's fees fare no better. Petitioners urge that, in calculating fee awards, courts may consider only the "direct benefit to the class," excluding *cy pres* amounts. That argument is outside the question presented and waived. Congress, moreover, specifically imposed that rule for *securities* class actions, but declined to impose it for class actions generally; petitioners seek to reverse that choice. Rule 23(h), which governs attorney's fees, requires fees to be "reasonable," affording courts broad discretion. Petitioners propose a categorical prohibition nowhere in the Rules.

III. Petitioners' policy arguments rest on the claim that plaintiffs' counsel "sell their putative clients down the river" to "self-deal," and that district courts are com-

plicit. But petitioners do not contend that happened here. The law forbids such behavior, which would violate fiduciary responsibilities. That courts occasionally misapply existing standards (often resulting in reversal) is no basis for judicially blue-penciling in proscriptions not found in the Rules' text.

IV. Petitioners hardly dispute that *this* settlement satisfies Rule 23(e). Petitioners ignore the settlement's prospective relief, which redresses the informed-consent concerns underlying the case. They concede Google's monetary payment is adequate. And their attack on the courts' factual findings—that distributing the fund was infeasible and that the recipients were selected on the merits—mischaracterizes the decisions below.

V. The government identifies a potential jurisdictional question regarding injury in fact. That counsels dismissing the petition as improvidently granted, particularly given the myriad other vehicle problems plaguing this case. In any event, the harms alleged here—privacy invasions—are the sort of non-pecuniary injuries long held actionable by courts.

ARGUMENT

The Federal Rules of Civil Procedure are promulgated through "an extensive deliberative process" that includes consideration by the Rules Advisory Committee, circulation for public comment, subcommittee review, consideration by the Judicial Conference, this Court's consideration, and submission to Congress. *Amchem Prods., Inc.* v. *Windsor*, 521 U.S. 591, 620 (1997). "The text of a rule thus proposed and reviewed limits judicial inventiveness. Courts are not free to amend a rule outside the process Congress ordered * * *." *Ibid.* Petitioners seek precisely such a judicial amendment here.

Nothing in Rule 23 or any other law supports petitioners' proposals. Their categorical prohibition on *cy pres* settlements has no textual basis. Petitioners' request that this Court pronounce new requirements for attorney's-fee calculations fares worse still. That request is not merely extra-textual; it is also not properly before this Court. Congress has adopted proposals like petitioners' for other contexts, but declined to impose them for class actions generally or for *cy pres* settlements specifically. Petitioners seek to overturn that deliberate choice. This Court "ha[s] no warrant to encumber [class-action] litigation by adopting an atextual requirement * * * that Congress, despite its extensive involvement in the * * * field, has not sanctioned." *Amgen Inc.* v. *Conn. Ret. Plans & Tr. Funds*, 568 U.S. 455, 478 (2013).

Under the standards set forth by the Federal Rules, *cy pres* settlements should be (and are) rare. The courts of appeals have converged on limited circumstances where such settlements can meet Rule 23's standards. Among other things, *cy pres* is appropriate only if distribution to class members is economically infeasible. Petitioners press their alternative of categorical prohibition by impugning the bar's integrity and denigrating the district courts' capabilities. But petitioners' generalized accusations have nothing to do with this case. They ignore or mischaracterize critical features of the settlement here—notably, the prospective relief it provides class members. And their complaints about misapplications of Rule 23's existing standards cannot justify rewriting the Rules by judicial fiat.

I. THE FEDERAL RULES AND RELEVANT STATUTES DO NOT PROHIBIT *CY PRES* SETTLEMENTS

The Federal Rules are construed using "'traditional tools of statutory construction,'" *Beech Aircraft Corp.* v.

Rainey, 488 U.S. 153, 163 (1988)—*i.e.*, their "text, structure, and history," *Kellogg Brown & Root Servs., Inc.* v. *United States ex rel. Carter*, 135 S. Ct. 1970, 1975 (2015). Petitioners appear to argue that *cy pres* cannot be "permitted at all" in class-action litigation. Pet. Br. 15. A settlement "that provides no direct benefit to the class," they urge, "cannot be approved." Pet. Br. 39. None of the "traditional tools of statutory construction" support reading that prohibition into Rule 23. And common sense defies it.

A. The Text, Structure, and History of Rule 23 Do Not Support Petitioners' Prohibition on *Cy Pres* Settlements

1. *Petitioners' Categorical Ban Defies Rule 23(e)'s Clear Text*

Under Rule 23(e), the "claims * * * of a certified class may be settled, voluntarily dismissed, or compromised only with the court's approval." Rule 23(e)(2) provides an express standard governing approval: "If the proposal would bind class members, the court may approve it only after a hearing and on finding that it is fair, reasonable, and adequate." That "general[] * * * standard" requires pragmatic balancing of "benefits and costs." *Nat'l Ass'n of Chain Drug Stores* v. *New Eng. Carpenters Health Benefits Fund*, 582 F.3d 30, 45 (1st Cir. 2005).

District courts must exercise sound "discretion" on "a case-by-case basis, in light of all the relevant circumstances." *Evans* v. *Jeff D.*, 475 U.S. 717, 742 (1986). Relevant factors include the "'strength of plaintiff's case on the merits balanced against the amount offered in the settlement,'" *Synfuel Techs., Inc.* v. *DHL Express (USA), Inc.*, 463 F.3d 646, 653 (7th Cir. 2006); and "'the range of reasonableness of the settlement fund'" in light of "'all the attendant risks'" of further litigation, *In re*

Prudential Ins. Co. Am. Sales Practice Litig., 148 F.3d 283, 317 (3d Cir. 1998).

Where Rule 23(e) establishes a generalized framework, petitioners propose a categorical rule: If the settlement "provides no direct or actual compensation to the class"—as opposed to injunctive relief or indirect benefits—it cannot be approved. Pet. Br. 20. But Rule 23(e) contains no such prohibition. Nor does it require class members to receive particular forms of relief such as cash. If Congress (or the Rules Advisory Committee or this Court) had intended such a prohibition, the Rule would state it. Courts "should be loath to announce * * * prohibitions that are unqualified by the statutory text." *Guidry* v. *Sheet Metal Workers Nat'l Pension Fund*, 493 U.S. 365, 376 (1990).

Petitioners' categorical preclusion sets Rule 23(e) on its head. Rule 23(e) permits resolutions where the class obtains *no relief at all*. A court may find that "voluntary dismissal" of class claims is "fair, reasonable, and adequate," Fed. R. Civ. P. 23(e), (e)(2), including a preclusive "voluntary dismissal *with prejudice*," Minutes, Meeting of the Advisory Committee on Civil Rules 25 (Apr. 23-24, 2001) (emphasis added). If dismissal of the class's claims with no relief can be "fair, reasonable, and adequate," *a fortiori* a settlement that provides prospective relief and a substantial payment to third parties—to be used for the class's benefit to address the legal wrongs prompting the suit—can be as well.

There are limited circumstances where a *cy pres* or injunctive-only remedy will meet Rule 23(e)'s requirements. But petitioners' across-the-board prohibition would be consistent with the Rule's text only if there were *no* such circumstances. That is not the case. Petitioners nowhere dispute that adverse legal and factual

developments during litigation may reduce the case's value to a point where any reasonable settlement amount is outstripped by the costs of distributing the proceeds to individual class members. In that situation, any rational class member would prefer an indirect benefit—from paying settlement proceeds to an organization that will serve their interests—to receiving *no* benefit at all. Petitioners nowhere explain why a settlement that brings class members *some benefit* and requires the defendant to pay *some recompense* is unfair, unreasonable, or inadequate, when the alternative is *nothing*.[4]

That is because petitioners' true goal in seeking a *cy pres* ban is to punish counsel for cases that work out poorly, to "discourage bad" lawsuits. Pet. Br. 43 (urging courts to force attorneys to "slink away and dismiss their cases"). But Rule 23(e) is about protecting "class members who have not participated in shaping the settlement," Fed. R. Civ. P. 23 advisory committee's note to 2003 amendment—not punishing counsel. The goal of deterring weak lawsuits is served by other provisions, including Rule 11, and context-specific fee-shifting statutes, *e.g.*, 15 U.S.C. §1692k(a)(3) (authorizing defense fees for certain Fair Debt Collection Act suits), to the fact that low-quality lawsuits most often result in costly investment for no return.

In non-class litigation, parties can reach voluntary resolutions that involve only forward-looking relief or pay-

---

[4] Petitioners hypothesize that counsel could negotiate a *cy pres* settlement but "opt out every single class member so that class members would obtain the settlement benefit while retaining their right to sue." Pet. Br. 53. That is implausible: Defendants typically require a "blow up provision" that scuttles the deal if too many plaintiffs opt out. 4 W. Rubenstein, *Newberg on Class Actions* §13:6 (5th ed.).

ments to third parties for the plaintiff's benefit. See, *e.g.*, *Beastie Boys* v. *Monster Energy Co.*, 983 F. Supp. 2d 369, 373 (S.D.N.Y. 2014) ($1 million payment "to a charitable organization chosen by the Beastie Boys and approved by [defendant]" to settle unauthorized use of band's song). As with other contracts, a promised performance under a settlement "may be given to the promisor *or to some other person*." *Restatement (Second) of Contracts* § 71(4) (1981) (emphasis added). Petitioners would preclude such arrangements for class actions alone, even where that is the best result obtainable for the class. But Rule 23 requires the settlement to be fair, reasonable, and adequate. That standard cannot possibly require courts to impose the less-adequate relief of *nothing* to replace the more-adequate relief of *something*.

2. *Petitioners' Categorical Ban Ignores Rule 23(e)'s Structure and History*

Since its inception, Rule 23(e) has provided a general standard governing settlement approval, not categorical prohibitions. As the Advisory Committee notes to the 2003 amendments observe, "many factors" may "deserve consideration," including those "provided by *In re: Prudential Ins. Co. American Sales Practice Litigation Agent Actions*, 148 F.3d 283, 316-324 (3d Cir. 1998)," and "found in the Manual for Complex Litigation." Petitioners' categorical prohibition on *cy pres* settlements is contrary to that approach, which entrusts district courts to exercise discretion in light of the totality of the circumstances.

Although *cy pres* settlements are rare, they date from shortly after Rule 23's modernization in 1966. See p. 8, *supra*. In the half-century since, Congress has repeatedly revisited class actions, implementing myriad changes. It considered *cy pres* settlements but never proscribed

them. For example, in 2005, Congress implemented extensive changes through the Class Action Fairness Act, Pub. L. No. 109-2, 119 Stat. 4. See pp. 6-7, *supra*. Congress specifically considered *cy pres* settlements. See, *e.g.*, *Class Action Fairness Act of 2003: Hearing on H.R. 1115 Before the H. Comm. on the Judiciary*, 108th Cong. 111-112 (2003); 151 Cong. Rec. S1,007-S1,008 (daily ed. Feb. 7, 2005) (statement of Sen. Hatch); S. Rep. No. 109-14, at 17, 19 (2005). But it did not preclude *cy pres*, even though it addressed other claimed abuses, such as "coupon settlements." See 28 U.S.C. § 1712(a). Quite the opposite. Congress empowered courts to "require" *cy pres* distributions in connection with coupon settlements: Under § 1712(e), district courts may "require that a proposed settlement agreement provide for the distribution of a portion of the value of unclaimed coupons to 1 or more charitable or governmental organizations" agreed upon by the parties. Congress treated *cy pres* as a useful tool—not an evil to be extirpated.

Congress has revisited the issue of *cy pres* settlements since. See *Class Actions Seven Years After the Class Action Fairness Act: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 112th Cong. 2, 40, 96 (2012); *State of Class Actions Ten Years After the Enactment of the Class Action Fairness Act: Hearing Before the H. Subcomm. on the Constitution & Civil Justice of the H. Comm. on the Judiciary*, 114th Cong. 10 (2015). Petitioners themselves have testified before Congress on *cy pres*. See *Examination of Litigation Abuses: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 113th Cong. 21-33 (2013); *Consumers Shortchanged? Oversight of the Justice Department's Mortgage Lending Settlements: Hearing Before the Subcomm. on Regulatory Reform*,

Commercial & Antitrust Law of the H. Comm. on the Judiciary, 114th Cong. 69-84 (2015). Congress's "silence on [that] issue, coupled with its certain awareness of" it, "is powerful evidence" of Congress's intent. *Wyeth* v. *Levine*, 555 U.S. 555, 575 (2009).

The House has passed a bill that would limit attorney's fees from *cy pres* settlements in class actions. See Fairness in Class Action Litigation and Furthering Asbestos Claim Transparency Act of 2017, H.R. 985, 115th Cong. § 1718. That proposal would make no sense if Rule 23(e) contained the absolute prohibition petitioners propose. This Court should not "adopt[ ] an atextual requirement * * * that Congress, despite its extensive involvement in the * * * field, has not sanctioned." *Amgen*, 568 U.S. at 478.

Nor does petitioners' prohibition find support elsewhere. Under CAFA, the Attorney General has been notified of any class-action settlement and been given the opportunity to interpose his views. 28 U.S.C. § 1715(a), (b), (d). The United States has often filed statements of interest. But it has never suggested that *cy pres* settlements are forbidden. U.S. Br. 1-2. The Rules Advisory Committee has considered *cy pres* settlements. A "[s]ubcommittee developed a fairly lengthy sketch of both a possible rule amendment and a possible Committee Note" to govern such settlements. *Report by the Committee on Rules of Practice and Procedure* 213 (2016). The subcommittee recommended against amending Rule 23 because, among other things, the circuits were converging around standards articulated by the American Law Institute. *Id.* at 213-214. The Advisory Committee thus did not understand Rule 23 to prohibit *cy pres* settlements—because it does not.

B. Federal Courts Have Identified the Limited Contexts Where *Cy Pres* Settlements Might Satisfy Rule 23(e)

Federal courts and commentators have, over the years, identified the narrow category of cases where a *cy pres* settlement may satisfy Rule 23(e)'s requirements. *First*, settlement funds must be so limited, and the cost of distributing the funds to class members so comparatively costly, that "distribution to the class members is infeasible" and would "provide no meaningful relief." *Hughes* v. *Kore of Ind. Enter., Inc.*, 731 F.3d 672, 675 (7th Cir. 2013); see *In re BankAmerica Corp. Sec. Litig.*, 775 F.3d 1060, 1064 (8th Cir. 2015); *In re Pharm. Indus. Average Wholesale Price Litig.*, 588 F.3d 24, 34 (1st Cir. 2009); *Klier* v. *Elf Atochem N. Am., Inc.*, 658 F.3d 468, 475 (5th Cir. 2011); *Masters* v. *Wilhelmina Model Agency, Inc.*, 473 F.3d 423, 436 (2d Cir. 2007). *Second*, *cy pres* recipients must truly serve the class-member interests pursued in the lawsuit. See, *e.g.*, *In re Baby Prods. Antitrust Litig.*, 708 F.3d 163, 175 (3d Cir. 2013); *In re Lupron Mktg. & Sales Practices Litig.*, 677 F.3d 21, 33 (1st Cir. 2012); *Six (6) Mexican Workers* v. *Ariz. Citrus Growers*, 904 F.2d 1301, 1308 (9th Cir. 1990). That requirement ensures that *cy pres* distributions actually, if indirectly, benefit the class. *Third*, courts must carefully review recipients to prevent conflicts of interests. See *Baby Prods.*, 708 F.3d at 173.

1. The "very best use" of settlement funds ordinarily is to pay them to "the class members directly." *Klier*, 658 F.3d at 475; see 4 *Newberg*, *supra*, § 12:26. Consistent with that, courts preclude *cy pres* distributions unless direct distribution to class members would be "infeasible." ALI Principles § 3.07 cmt. b. "Infeasible" means that "distributions are [not] sufficiently large to

make individual distributions economically viable." *Id.* §3.07(a).

Direct distribution to class members is rarely infeasible. But sometimes unclaimed funds may be too limited to warrant distribution. See 4 *Newberg*, *supra*, §12:32. Or it may become apparent during litigation that the risk-discounted value of a case—and the maximum the defendant will pay in settlement—has become "too small" to support the expense of the claims-administration system necessary to send a "recovery to individuals." *Pharm. Indus.*, 588 F.3d at 34. The costs of claims processing—providing notice, distributing and receiving claims forms, verifying claims, and distributing proceeds—can be prohibitive. Consequently, where the settlement value of the case is small and the class is very large, especially where class members are not readily identifiable, the costs of distributing settlement funds could dwarf any recovery. *Holtzman* v. *Turza*, 728 F.3d 682, 689 (7th Cir. 2013); *New York* v. *Reebok Int'l Ltd.*, 96 F.3d 44, 49 (2d Cir. 1996).

In those limited circumstances, *cy pres* distribution to an organization that will serve class-member interests can be "the best solution." *Hughes*, 731 F.3d at 675. The "indirect benefit to the class" that results from *cy pres* distribution, *Klier*, 658 F.3d at 475, may satisfy Rule 23(e) as a "fair, reasonable, and adequate" resolution, see *Hughes*, 731 F.3d at 675; *Baby Prods.*, 708 F.3d at 173-174; *Klier*, 658 F.3d at 475; *Pharm. Indus.*, 588 F.3d at 34; *Powell* v. *Ga.-Pac. Corp.*, 119 F.3d 703, 706-707 (8th Cir. 1997); *Reebok*, 96 F.3d at 49. "A foundation that receives $10,000 can use the money to do something to minimize violations" of the law at issue. *Hughes*, 731 F.3d at 676. But class members who receive checks for a dollar cannot. *Ibid.*; see *In re MGM Mirage Sec. Litig.*, 708 F.

App'x 894, 897 (9th Cir. 2017) (citing "evidence showing that smaller checks, such as those under $10, in many instances are never cashed").

A *cy pres* settlement serves class members' interests in deterring misconduct. It "'[p]revents the defendant from walking away from the litigation' without paying a full recovery" simply because there are "practical obstacles to individual distribution." *Pharm. Indus.*, 588 F.3d at 33-34. Deterring future misconduct, and ensuring the defendant provides *some* remedy, is particularly salient where the violations concern privacy or other non-pecuniary harms. In those instances, the indirect benefits of *cy pres* may better redress the injury than would a tiny check.

2. Courts also require that *cy pres* payments fund activities that serve the class-member interests pursued in the suit. ALI Principles §3.07(c). The proposed recipient must seek to rectify a problem "tethered to the nature of the lawsuit," so as to advance "the interests of the silent class members." *Nachshin* v. *AOL, LLC*, 663 F.3d 1034, 1039 (9th Cir. 2011); see *Lupron*, 677 F.3d at 33; *Baby Prods.*, 708 F.3d at 180 n.16. That requirement ensures that the *cy pres* distribution "provid[es] an indirect benefit to the class." *Klier*, 658 F.3d at 475; *Mexican Workers*, 904 F.2d at 1308.

3. Finally, the resolution must avoid appearances of impropriety or self-dealing. *Cy pres* is inappropriate "if the court or any party has any significant prior affiliation with the intended recipient that would raise substantial questions about whether the selection of the recipient was made on the merits." ALI Principles §3.07 cmt. b. That standard ensures fairness—actual and perceived—to absent class members. See Pet. App. 14.

4. Far from disputing those principles, petitioners endorse many. Petitioners support an infeasibility standard (at 49), declaring that *cy pres* is "inappropriate * * * if it is feasible to distribute cash." They endorse the ALI's standards governing affiliations between a party and *cy pres* recipients. Pet. Br. 55-56 (citing ALI Principles §3.07 cmt. b.). There is good reason for that agreement: Proper application of those principles precludes the putative abuses on which petitioners rest their case. See pp. 43-46, *infra*. Courts reviewing settlements under Rule 23(e)'s "fair, reasonable, and adequate" standard already apply those principles rigorously to limit *cy pres* settlements to the unusual circumstances where it is the best way to serve class-member interests.

Petitioners propose modifying those principles. They contend that, even if it is "prohibitively expensive to distribute money to every claimant" in the class, distribution is not infeasible where the district court could conduct "random lottery distribution to" some "percentage of claiming class members." Pet. Br. 44, 51. But the lottery reduces claims-processing costs very little: The class still must be given notice of the lottery and means of entering; claims must be verified; and some number of winners must be sent their winnings. The lottery system addresses only one cost (final mailing of checks) of myriad administrative costs that might dwarf any recovery.

A lottery, moreover, intentionally denies some class members any benefit to increase the return for others. But Rule 23(e)'s "fairness" standard involves "a comparative analysis of the treatment of class members vis-à-vis each other." Fed. Jud. Ctr., *Manual for Complex Litigation* (4th) §21.62 (2004) (cited in Fed. R. Civ. P. 23 advisory committee's note to 2003 amendment). A lottery treats them differently based on a mechanism that is con-

cededly "arbitrary." Pet. Br. 44. A judicially backed mega-millions lottery might increase public participation, but it is unseemly to benefit some by denying any benefit to others. And petitioners nowhere explain why a lottery "would necessarily result in greater relief to the class as a whole than a properly tailored *cy pres* award." U.S. Br. 27 n.2.

The ultimate question is not whether a lottery might be permissible. It is whether a district court abuses its discretion by not mandating one. If direct compensation of class members is not feasible, nothing in Rule 23(e) requires a court to select a lottery "next best" proposal for distributing funds over the long-recognized *cy pres* alternative.

C. Rule 23(b)(3)'s "Superiority" Requirement Does Not Preclude *Cy Pres* Resolution

Finding nothing in Rule 23(e) to support their categorical ban, petitioners turn to Rule 23(b)(3). If class members cannot receive direct monetary compensation, they urge, the proposed class cannot satisfy Rule 23(b)(3)'s "superiority" requirement. Pet. Br. 52-54; see Ariz. Br. 9-10. In such cases, they assert, "retaining [an individual] right to sue" is superior. Pet. Br. 53.

1. Rule 23(b)(3) requires that class treatment be "superior *to other* available methods *for fairly and efficiently adjudicating the controversy*." Fed. R. Civ. P. 23(b)(3) (emphasis added). Where individual claims have little value—as is true in any case eligible for *cy pres* resolution—the class members "would have no realistic day in court if a class action were not available." *Phillips Petrol. Corp.* v. *Shutts*, 472 U.S. 797, 809 (1985). "The *realistic* alternative to a class action is not 17 million individual suits, but zero individual suits, as only a lunatic

or a fanatic sues for $30"—or $1. *Carnegie* v. *Household Int'l, Inc.*, 376 F.3d 656, 661 (7th Cir. 2004).

Petitioners thus seek to foreclose class actions precisely where the Rules promote them. "'The policy at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights.'" *Amchem*, 521 U.S. at 617.

2. The government urges that, "[e]ven if the alternative to a class action is that the plaintiff would not bring a lawsuit at all, a class action that yields no relief is still not 'superior' to that alternative." U.S. Br. 26. That is mistaken. *First*, the Rule's *text* directs courts to ask whether class treatment is superior to "alternative means of adjudicating"—not to compare class adjudication with no adjudication.

Second, the government incorrectly assumes that *cy pres* settlements "yield no relief." Here, there was direct, prospective relief for the class—disclosures to avoid unconsented sharing of stored communications—to forestall future violations. And any *cy pres* settlement that meets Rule 23(e)'s "fair, reasonable, and adequate" standard yields relief, even if benefits are indirect. *Cy pres* recipients must "'serve the objectives of compensation for the class,'" and the payment "'deter[s] * * * illegal behavior,'" preventing the defendant from "'walking away from the litigation'" with no reckoning. *Pharm. Indus.*, 588 F.3d at 33. Class members surely would prefer those benefits to the government's proffer of *nothing*.

Third, the notion that "superiority" disappears whenever the case yields insufficient relief is fundamentally misconceived. Under that view, classes would have to be decertified whenever plaintiffs *lose*—in such cases, class

members get "no relief." But the merits of the case and the ultimate outcome are irrelevant to superiority. See *Eisen* v. *Carlisle*, 417 U.S. 156, 177 (1974).

D. Petitioners' and Their *Amici*'s Remaining Arguments Fail

1. *Petitioners' First Amendment Argument Is Waived and Meritless*

In one paragraph, petitioners suggest that *cy pres* settlements "raise[ ] serious First Amendment concerns," because recipients might "have political valence[s] * * * offensive to * * * class members." Pet. Br. 36-37. Petitioners never mentioned the First Amendment in the court of appeals, and the court never addressed it. This Court will not address issues "neither raised in nor passed upon by the Court of Appeals." *Glover* v. *United States*, 531 U.S. 198, 205 (2001). The First Amendment is not within the question presented (which concerns Rule 23 standards). And it appears nowhere in the petition for certiorari. That forecloses its consideration here. See *Bay Area Laundry & Dry Cleaning Pension Tr. Fund* v. *Ferbar Corp. of Cal., Inc.*, 522 U.S. 192, 206-207 (1997); *Granite Rock Co.* v. *Int'l Bhd. of Teamsters*, 561 U.S. 287, 306 (2010).

The argument fails in any event. Petitioners fail to address the state-action requirement, a pre-requisite to any First Amendment claim. *In re Motor Fuel Temperature Sales Practices Litig.*, 872 F.3d 1094, 1113-1114 (10th Cir. 2017) (holding that judicial approval does not convert private settlement agreements into state action). Besides, the short answer for anyone with genuine objections to a *cy pres* recipient—or to the lawsuit—is to opt out. That opportunity protects due process rights, *Phillips*, 472 U.S. at 810-814, and First Amendment interests, cf. *Christian Legal Soc'y Chapter of Univ. of*

Cal. v. *Martinez*, 561 U.S. 661, 682 (2010) (distinguishing "regulations that *compelled* a group to include unwanted members, with no choice to opt out," from a policy with opt-out mechanism).

2. Cy Pres *Raises Neither Redressability Nor Rules Enabling Act Concerns*

The government urges that *cy pres* settlements raise Article III issues because they might not "redress" the plaintiffs' injuries. U.S. Br. 22-25. The argument has no application in this case: The settlement here provides for *prospective relief* that alters the defendant's behavior to redress the injury alleged. The wrong asserted by the complaint was use of private information without consent. See p. 11, *supra*. The settlement requires Google to make permanent changes to its disclosures so that users know of, and consent to, such uses. See pp. 48-49, *infra*. That relief precisely addresses, and remedies, the wrong alleged. The government does not suggest otherwise.

The government raises the hypothetical concern that, where the only relief is a *cy pres* payment, that might not "redress[ ] plaintiffs' injuries." U.S. Br. 22. But "redressability," as an element of standing, depends on the relief sought, not the ultimate settlement terms chosen. No authority supports the government's contrary position. *Motor Fuel*, 872 F.3d at 1114.[5] Monetary payments,

---

[5] The government cites no case suggesting that settlement terms might retroactively render an injury non-redressable. See *United States* v. *Sanchez-Gomez*, 138 S. Ct. 1532, 1537-1538 (2018) (reviewing mootness); *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 559 (1992) (reviewing grant of motion to dismiss); *Steel Co.* v. *Citizens for a Better Env't*, 523 U.S. 83, 88 (1998) (same); *Friends of the Earth, Inc.* v. *Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 173 (2000) (litigated judgment on the merits); *City of Los Angeles* v. *Lyons*, 461 U.S. 95, 98-99 (1983) (same); *Gill* v. *Whitford*, 138 S. Ct. 1916, 1924-

moreover, are given "to *substitute* for a suffered loss," not to repair the injury itself. *Bowen* v. *Massachusetts*, 487 U.S. 879, 895 (1988). Outside the class-action context, parties can voluntarily redirect that substitute to third parties. See pp. 27-28, *supra*. The government nowhere explains why Article III operates differently for class actions. Besides, under the ALI standards applied here, third-party recipients must apply the funds to benefit class members and address the specific injuries that prompted suit. See pp. 31-33, *supra*. That is redress.

Nor do *cy pres* settlements violate the Rules Enabling Act or expand substantive remedies. Pet. Br. 33, 38; Ariz. Br. 10-11. Settlement agreements are contracts. A district court's approval "simply recognizes the parties' deliberate decision to bind themselves according to mutually agreed-upon terms without engaging in any substantive adjudication" of the merits. *Sullivan* v. *DB Invs., Inc.*, 667 F.3d 273, 312 (3d Cir. 2011). Because it makes no "finding that plaintiffs are actually entitled to relief under substantive * * * law, * * * a court does not 'abridge, enlarge, or modify any substantive right' by approving a voluntarily-entered class settlement agreement." *Id.* at 313 (quoting 28 U.S.C. §2072(b)); accord *Marshall* v. *Nat'l Football League*, 787 F.3d 502, 511 n.4 (8th Cir. 2015); *Baby Prods.*, 708 F.3d at 173 n.8; *Mexican Workers*, 904 F.2d at 1307.

If anything, petitioners' contrary view raises Rules Enabling Act concerns. No law precludes non-class suits from being settled on terms that include third-party payments. Yet petitioners read the Federal Rules to impose that substantive prohibition on class actions.

1925 (2018) (same); *Califano* v. *Yamasaki*, 442 U.S. 682, 688-690 (1979) (same).

II. Petitioners' Proposed Attorney's Fees Rules Are Misplaced And Unfounded

Petitioners devote much of their brief to proposals regarding attorney's-fee calculations. See Pet. Br. 20-49, 56-57. Those proposals are not properly before the Court. None is supported by Rule 23.

A. Petitioners' Attorney's Fees Proposals Are Not Properly Before the Court

Petitioners "ask this Court to hold" that attorney's fees, for "*all* Rule 23 settlements," may reflect only the "actual and direct benefit to the class." Pet. Br. 15, 48 (emphasis added). But the question presented does not encompass that request. Petitioners limited the question presented to "*a cy pres award* of class action proceeds." Pet. i (emphasis added). It does not address class actions generally.

The question presented, moreover, asks whether a *cy pres* settlement that affords no direct monetary relief to class members "comports with" Rule 23(*e*)'s "requirement that a settlement binding class members must be '*fair, reasonable, and adequate*,'" or "supports *class certification*" under Rule 23(*b*). Pet. i (emphasis added). That does not encompass fee awards, which are governed by 23(*h*)'s requirement that fees be "reasonable."

Petitioners' fee arguments, moreover, were waived below. In district court, petitioners never argued that fee-award calculations must exclude *cy pres* distributions. Petitioners urged the district court to limit fees to "no more than 10%" of the fund. Pet. App. 139. The court of appeals did not pass on petitioners' argument for excluding *cy pres* payments, presumably because of that waiver. This Court should not entertain arguments not preserved or passed upon below. *Taylor* v. *Freeland &*

Kronz, 503 U.S. 638, 645-646 (1992). Applying a new rule "without the benefit of a full record or lower court determinations is not a sensible exercise of this Court's discretion." *Lytle* v. *Household Mfg., Inc.*, 494 U.S. 545, 551 n.3 (1990).

B. Petitioners' Fee Rules Defy Text and History

Rule 23(h) permits "reasonable" attorney's fees, a standard that affords district courts considerable discretion. See 7B C. Wright & A. Miller, *Federal Practice and Procedure* § 1803.1 (3d ed.). One important consideration is the degree of success. Fed. R. Civ. P. 23 advisory committee's note to 2003 amendment. Consequently, to the extent indirect benefits from a *cy pres* settlement bring less value, courts already have ample "case by case" discretion "to decrease attorneys' fees where a portion of a fund will be distributed *cy pres*." *Baby Prods.*, 708 F.3d at 179. Conversely, "[c]lass counsel should not be penalized for * * * reasons unrelated to the quality of representation," and district courts have discretion not to impose such discounts. *Id.* at 178.

Dissatisfied by Rule 23(h)'s flexible "reasonable[ness]" standard, petitioners insist on a categorical rule: Courts must "*exclude[]* * * * *cy pres* awards from the calculation," counting only the "direct benefit to the class." Pet. Br. 15, 40 (emphasis added). Rule 23 contains no such command. In *Boeing Co.* v. *Van Gemert*, 444 U.S. 472 (1980), this Court refused to blue-pencil a similar prohibition into the Rule, declining to hold that courts cannot base fees on "the unclaimed portion" of a recovery. *Id.* at 477-478. The plaintiffs' attorneys had "recovered a determinate fund for the benefit of every member of the class whom they represent," which merited consideration even though some portion remained unclaimed. *Id.* at 479-482. Because *Boeing* "confronted

essentially the same issue" petitioners raise here, it all but forecloses "requiring district courts to discount attorneys' fees when a portion of an award will be distributed *cy pres*." *Baby Prods.*, 708 F.3d at 177-178; see *Mexican Workers*, 904 F.2d at 1311.

Moreover, Congress has twice enacted legislation tying attorney's fees to "direct benefits" in other contexts. CAFA limits fees for *coupon settlements* to "the value to class members of the coupons that are redeemed." 28 U.S.C. § 1712(a). The PSLRA limits fees *in securities cases* to "a reasonable percentage of the amount of any damages and prejudgment interest actually paid to the class." 15 U.S.C. § 77z-1(a)(6). But Congress has not imposed that rule for class actions generally or *cy pres* specifically—despite considering *cy pres* extensively. See pp. 9-11, *supra*. Congress's decision to limit or exclude recoveries from fee calculations only in specific contexts forecloses the broader rule that petitioners demand here.[6]

---

[6] Petitioners' effort to insert an extra-textual exclusion into attorney's-fee calculations is particularly misplaced given changes proposed by the Rules Advisory Committee. As that Committee recently confirmed, "any award of attorney's fees must be evaluated under Rule 23(h), and no rigid limits exist for such awards." Fed. R. Civ. P. 23 advisory committee's note to 2018 amendment. The Committee approved amendments to Rule 23(e) requiring courts to consider "the terms of any proposed award of attorney's fees" in connection with whether the "relief provided for the class [in the settlement] is adequate." Fed. R. Civ. P. 23(e)(2)(C)(iii) (effective Dec. 1, 2018, absent congressional action). That general directive is inconsistent with the categorical exclusion petitioners seek. And the fact that new Rules become effective December 1, 2018, makes consideration of fee issues resolved under the current but soon-to-be-superseded Rules rather pointless.

III. Petitioners' Policy Arguments Fail

Petitioners' arguments are based not on text, structure, or history, but policy. Petitioners accuse the bar of unethical conduct and the courts of dereliction of duty. According to petitioners, plaintiffs' counsel "enrich[ ]" themselves "at the expense of their clients," "sell their putative clients down the river," and engage in "self-deal[ing]," "gimmicks," "subterfuge," and "gamesmanship." Pet. Br. 16, 20-21, 22, 29, 40, 48.[7] Defendants are accused of "conniv[ing]" with plaintiffs. Pet. Br. 30-33, 40. Petitioners' dim view extends to the judiciary as well. District courts, we are told, "ignor[e] and resist[ ] circuit court" guidance, or seek to benefit favored charities. Pet. Br. 37, 49. Those accusations are unfounded. And existing rules amply proscribe the conduct that petitioners impute to their brethren.

A. Existing Standards Address Petitioners' Concerns

Attorneys have "solemn dut[ies]" to "advance the interests of [their] client[s]." *Nix* v. *Whiteside*, 475 U.S. 157, 168 (1986). They "are personally subject to an ethical regime designed to reinforce the profession's standards." *Connick* v. *Thompson*, 563 U.S. 51, 65 (2011). Petitioners presume misconduct where this Court should not. The Court will not rewrite the Federal Rules "premised on the assumption that in the pursuit of fees, attorneys will choose to bring claims lacking good faith or a reasonable basis in derogation of their ethical duties." *Sebelius* v. *Cloer*, 569 U.S. 369, 382 (2013).

---

[7] See Pet. Br. 1 ("minimize payoff by the defendant, maximize benefit to class counsel, and leave injured class members out in the cold"), 19 ("illusory settlement at class members' expense"), 22 ("obscuring * * * allocative decisions" to "trade benefits to defendants for bigger fees").

Rule 23's proper application precludes the misconduct on which petitioners base their arguments. Under Rule 23(e), courts must reject any settlement that is not "fair, reasonable, and adequate." District courts rigorously enforce the rule; appellate courts step in where district courts misapply the law. See, *e.g.*, *In re Dry Max Pamper. Litig.*, 724 F.3d 713, 718-719 (6th Cir. 2013); *Koby* v. *ARS Nat'l Servs., Inc.*, 846 F.3d 1071, 1080 (9th Cir. 2017); *In re Airline Ticket Comm'n Antitrust Litig.*, 268 F.3d 619, 625-626 (8th Cir. 2001).

Rule 23(e) is regularly invoked to reject ordinary settlements that courts deem inadequate. See, *e.g.*, *In re Subway Footlong Mktg. Litig.*, 869 F.3d 551, 556-667 (7th Cir. 2017); *Koby*, 846 F.3d at 1079; *Polar Int'l Brokerage Corp.* v. *Reeve*, 187 F.R.D. 108, 112 (S.D.N.Y. 1999). The *cy pres* context is no different: Petitioners' own brief cites at least five cases where courts rejected a proposed *cy pres* settlement as inadequate, requiring counsel to obtain more money that could be distributed to the class. See Pet. Br. 42-43 (citing *Baby Prods.*, 708 F.3d at 178; *Fraley* v. *Facebook, Inc.*, 966 F. Supp. 2d 939, 939 (N.D. Cal. 2013); *In re Bayer Corp. Litig.*, No. 09-md-2023, 2013 WL 12353998, at *3 (E.D.N.Y. Nov. 8, 2013); *Pecover* v. *Elec. Arts Inc.*, No. 08-cv-02820, 2013 WL 12121865 (N.D. Cal. May 30, 2013); *Pearson* v. *NBTY, Inc.*, No. 11-cv-07972, Dkt. 213-1 (N.D. Ill. May 14, 2105)). Contrary to petitioners' suggestion, "experience" has "borne out," Pet. Br. 42, that *cy pres* settlements are "rejected when the proposed distribution fails" to satisfy Rule 23's standards, *Mexican Workers*, 904 F.2d at 1308.

Petitioners' accusation that defendants use *cy pres* to "benefit themselves," Pet. Br. 30-33, founders. Petitioners invoke *In re Microsoft Corp. Antitrust Litigation*, 185 F. Supp. 2d 519 (D. Md. 2002), to accuse Microsoft of

having "attempted to resolve an antitrust class action by directing a *cy pres* donation of computers and software to schools" to give itself a business advantage. Pet. Br. 31. Petitioners omit that the district court *rejected* the proposed settlement for that very reason. See *Microsoft*, 185 F. Supp. 2d at 528-530.

While the government invokes the "'risk of collusion' between the parties at the expense of absent class members," U.S. Br. 19, absentees' interests are protected by existing rules. Courts demand "rigorous adherence to those provisions of [Rule 23] 'designed to protect absentees,'" *Ortiz* v. *Fibreboard Corp.*, 527 U.S. 815, 849 (1999) (quoting *Amchem*, 521 U.S. at 620)—including Rule 23(e)'s fair, reasonable, and adequate standard, see Fed. R. Civ. P. 23 advisory committee's note to 2003 amendment. Class counsel also have fiduciary obligations. Rule 23(a)(4) requires them to fairly and adequately represent the interests of the class in all cases, whether they involve *cy pres* or not. See *Ortiz*, 527 U.S. at 856-857; *Gallego* v. *Northland Grp. Inc.*, 814 F.3d 123, 129 (2d Cir. 2016). And for settlement-only classes, courts apply even greater scrutiny to guard against collusion. *Hanlon* v. *Chrysler Corp.*, 150 F.3d 1011, 1026 (9th Cir. 1998).

Unwilling to address the actual rules, petitioners attack the courts. Petitioners urge that district courts face "conflicts of interest" in *cy pres* settlements, and "resist[]" precedent confining their authority. Pet. Br. 37, 49. Not so: Courts typically avoid injecting their interests into *cy pres* recipient selection by leaving it to the parties. See ALI Principles §3.07(c). Courts of appeals "greet[] with * * * skepticism *cy pres* distributions imposed by trial courts." *Baby Prods.*, 708 F.3d at 172 n.7. Widely accepted standards prevent the appearance

of impropriety in selecting recipients, ALI Principles §3.07 cmt. b., and "there are objective standards that require recusal" in appropriate circumstances, *Caperton* v. *A. T. Massey Coal Co.*, 556 U.S. 868, 872 (2009). This Court should not legislate new rules where proper application of existing ones amply addresses petitioners' accusations.

Finally, petitioners urge that the potential for a *cy pres* settlement encourages "strike" suits. Pet. Br. 36. They offer no economic analysis to support that claim. "[T]he existence of a cy pres component, by itself, should not adversely affect the total settlement. Since the attorney's fee depends on the total amount, the class attorney has an incentive to maximize the total." R. Bone, *Justifying Class Action Limits: Parsing the Debates over Ascertainability and Cy Pres*, 65 U. Kan. L. Rev. 913, 945-946 (2017). And "the class attorney does not benefit in any obvious way by directing proceeds to a cy pres beneficiary rather than to the class; her fee is the same in either case." *Ibid.* The fact that *cy pres* settlements are rare belies petitioners' supposition that they encourage unfounded suits. See p. 9, *supra*. Strike suits should be deterred by rigorous application of legal provisions designed to prevent them—not by judicial imposition of categorical rules to preclude the occasional *cy pres* settlement.[8]

B. Petitioners' Accusations Are Unfounded

Petitioners' argument rests on a parade of horribles that presumes defiance of settled norms. Pet. Br. 33-35

---

[8] Petitioners' arguments (at 35) about *cy pres* permitting class treatment of otherwise unmanageable cases fails for the same reason. This Court has rejected the notion that a settlement class must be manageable through trial. See *Amchem*, 521 U.S. at 620.

& n.3, 37-38; U.S. Br. 25; Cato Br. 15. But the parade reduces to a procession of worn-out floats. Petitioners invoke *Nachshin*, 663 F.3d 1034, as a case where the judge "select[ed] [the] judge's spouse's charity as [a] *cy pres* recipient." Pet. Br. 38. But *Nachshin* reversed the approval. 663 F.3d at 1040. The accusation, moreover, is unfair: The charity was suggested by a *mediator*, and the judge's sole connection was that her spouse sat on its *50-person* board. *Id.* at 1041-1042. That tenuous connection provided no ground for recusal under the governing statute. *Ibid.* (applying 28 U.S.C. § 455).

Petitioners invoke cases in which they and others challenged the settlement, but then dismissed their appeals. Pet. Br. 31, 34, 37.[9] Petitioners thus ask this Court to pronounce on those settlements without prior consideration in a court of appeals. And petitioners scrape the bottom of the barrel when they invoke an aged press release about a *state-court* settlement to support a judicial rewrite of the Federal Rules. Pet. Br. 34 (discussing state-court Rezulin suit).

There are undoubtedly cases where Rule 23's standards were not applied with appropriate rigor. But the same can be said of *any* Federal Rule (or substantive law). That occasional result hardly justifies judicial insertion of new prohibitions that Congress has declined to impose.

---

[9] Petitioner dismissed his appeal in *Citigroup*, see *ATD Grp.* v. *Frank*, No. 16-2850, 2017 WL 4014951 (2d Cir. Mar. 29, 2017) (cited Pet. Br. 34), as did the objector in *In re Google Buzz Privacy Litig.*, No. 11-16587 (9th Cir. Nov. 21, 2011), ECF No. 14 (cited Pet. Br. 31, 34, 37).

IV. This Settlement Complies With Rule 23

After extensive hearings and carefully considering petitioners' objections, the district court found the settlement "fair, reasonable, and adequate." Fed. R. Civ. P. 23(e)(2); see Pet. App. 39-52; pp. 16-18, *supra*. Notwithstanding petitioners' fact-bound contentions, the court committed no abuse of discretion.

A. The Settlement Provides Valuable Prospective Relief To Prevent Violations

The settlement includes prospective relief requiring new, permanent changes to Google's disclosures—changes that would apprise users of, and allow them to make informed choices regarding, Google's use of referrer headers. Pet. App. 49-50. Those disclosures make clear that user "search queries [are] sent to websites when [users] click on Google Search results." Pet. App. 109-111. That redresses the legal violation at the center of the suit, which was Google's use of information without informed consent. See J.A. 35-36; 18 U.S.C. §2702(b)(3) (permitting disclosure of electronic communications only with "lawful consent"). In its final approval order, the district court noted the value of that "injunctive relief." Pet. App. 50. Google was now "obligated to make * * * changes to * * * better inform users how their search terms could be disclosed to third parties." J.A. 94.

While petitioners refer to the settlement as "*cy pres* only," that is incorrect: The class received the direct benefit of prospective relief to stop the violations that prompted the suit. As the district court held, "contrary to what the objectors argue, future users of Google's website will receive something from the injunctive relief: the capability to better understand Google's disclosure practices before conducting a search." Pet. App. 50. Petitioners' suggestion that Google merely agreed to

"continue to include" disclosures already being made, Pet. Br. 9, is false. The settlement required "additional disclosures." Pet. App. 73. Petitioners admitted as much in their certiorari petition, representing that Google was obligated to "*revise* its 'Frequently Asked Questions' webpages." Pet. 9 (emphasis added). The record on that point is undisputed. J.A. 38 (class counsel explaining that Google was "going to make their disclosures more robust and more prominent"). The settlement imposed "permanent prospective relief requiring disclosures from Google," a "change" from prior practice. J.A. 145-147.

B. The District Court Properly Found the Cash Component Adequate and Non-Distributable

The settlement included a payment of $8.5 million. The district court found that payment adequate given the "significant and potentially case-ending" legal developments after the suit was filed. Pet. App. 58-59. Petitioners do not dispute the payment's adequacy. Despite claiming that plaintiffs' counsel sell their clients out, petitioners never claimed that happened here. To the contrary, they opined that perhaps "Google is overpaying." J.A. 118.

The district court recognized that even limited funds must be distributed to class members unless distribution would be infeasible. See Pet. App. 45-47. The court found it infeasible to distribute the fund here given that the class size "exceeds one hundred million individuals." Pet. App. 47; J.A. 33.[10] Even before deducting *any* administration costs or attorney's fees, the $8.5 million fund amounted to only 6.5 cents per class member. Experi-

---

[10] According to comScore, which provides website analytics, 129.9 million people visited Google's search website in the six months preceding the motion for preliminary settlement approval. J.A. 87 n.2.

enced in handling class actions, the district court understood that the costs of notice, claim processing, claim verification, and distribution would make "actual remuneration * * * to an individual class member * * * virtually impossible." J.A. 33. "[R]equiring proofs of claim" from such a class "would impose a significant burden to distribute, review and then verify." J.A. 95-96. "[T]he cost of sending out very small payments to millions of class members would exceed the total monetary benefit obtained by the class." Pet. App. 47; see J.A. 95-96 (same). The class "potentially covers all internet users in the United States," so "direct notice to class members * * * is impractical." J.A. 98. Notice of the settlement alone cost about $855,000—over 10% of the settlement fund. C.A. S.E.R. 152-161, 232-233.[11]

This Court does "not inspect and set aside for insufficient evidence District Court findings of fact," *Amchem*, 521 U.S. at 622 n.17, especially findings "accepted by two lower courts," *Tex. Dep't of Hous. & Cmty. Affairs* v. *Inclusive Cmtys. Project, Inc.*, 135 S. Ct. 2507, 2544 (2015). Petitioners therefore recharacterize the decisions below as announcing a legal rule: that *cy pres* is permissible any time the fund, divided by the class size, yields a small quotient. Pet. Br. 49-52; cf. U.S. Br. 27-28. But the courts below never held that *cy pres* is permitted whenever a settlement fund cannot "be distributed to *every*

---

[11] This is not a case where class members could be identified and money distributed based on existing relationships. Contrast *In re Online DVD-Rental Antitrust Litig.*, 779 F.3d 934, 940 (9th Cir. 2015) (subscriber list); *McDonough* v. *Toys "R" Us, Inc.*, 80 F. Supp. 3d 626, 636 (E.D. Pa. 2015) (purchase records). Here, "it would not be possible for Google to direct payment to any significant proportion of class members" without a claims process. Google Br. 36, *In re Google Referrer Header Privacy Litig.*, No. 15-15858 (9th Cir. Dec. 4, 2015), ECF No. 26.

potential class member." Pet. Br. 15, 18. The Ninth Circuit affirmed what the district court "found": "that the cost of verifying and 'sending out very small payments to millions of class members would exceed the total monetary benefit obtained by the class.'" Pet. App. 9. That finding rests not on a mathematical rule, but on an experienced district judge's case-specific evaluation. Even if there were just a 2% claims rate, notice to the class, claims processing, verification, and distribution would at most leave dimes for each claimant, not dollars. Pet. App. 5.[12]

Petitioners insist that the district court was *required* to reject the settlement based on speculation that fewer class members might file claims. Pet. Br. 44-45; see pp. 34-35, *supra* (addressing lottery). But class actions with big-name defendants, coupled with effective notice mechanisms, yield higher claims rates. Underestimating the claims rate would mean dissipating the fund on processing. District courts have discretion in applying Rule 23, and "[d]iscretion means a choice" among permissible options. *United States* v. *Paramount Pictures, Inc.*, 334 U.S. 131, 179 (1948); *Gallego*, 814 F.3d at 128-129. In some cases, *pro rata* distribution to claimants might make sense. But it makes no sense to *require* it where notice, claims processing, verification, and payment costs would exceed any benefit to the class.

---

[12] Even at just 2% participation (2.59 million claimants), and claims-administration costs of only $1.50 per claimant (an unrealistically low estimate given the difficulty of identifying class members and the need to mail checks), administration costs would absorb at least $3.89 million of the $5.3 million available. See *In re Wells Fargo Secs. Litig.*, 991 F. Supp. 1193, 1196 & n.1 (N.D. Cal. 1998) (costs of $1.50 to $5.50 per claimant). That would leave only 54 cents per claimant—more likely less, potentially zero.

C. The District Court Did Not Abuse Its Discretion in Approving Recipients

Under ALI principles followed below, *cy pres* recipients must use the funds to address the types of injury that class members suffered. ALI Principles §3.07(c); see, *e.g.*, *Lupron*, 776 F.3d at 33; *Baby Prods.*, 708 F.3d at 180; see pp. 31-33, *supra*. Petitioners never argue that the recipients here fail that test. See Pet. App. 12 ("Objectors do not dispute that the nexus requirement is satisfied here."). Nor could they: The *cy pres* recipients provided detailed proposals specifying their use of funds. App., *infra*, 9a-223a.

Petitioners urge that recipient selection was affected by counsel's allegiances. Pet. Br. 54-56. There is no dispute, however, over the relevant standard. Counsel should not "'have any significant prior affiliation with the intended recipient that would raise substantial questions about whether the selection of the recipient was made on the merits.'" Pet. Br. 55-56 (quoting ALI Principles §3.07 cmt. b). The court of appeals applied that standard to reject petitioners' arguments. Pet. App. 14 (quoting ALI Principles §3.07 cmt. b).

This Court need not reconsider petitioners' fact-bound complaint that, of the six *cy pres* recipients, three were housed at schools attended by class counsel (Harvard, Stanford, and Chicago-Kent). Pet. Br. 54-55. Counsel made clear they had no connection to those schools beyond having attended them: As one explained, "I simply got my law degree [at Harvard], and that's simply the end of it." Pet. App. 19 (quoting J.A. 136). That belies petitioners' assertion (at 11) that counsel failed to "deny that the *alma mater* status played a part in their selection." The district court found "*no indication* that counsel's allegiance to a particular alma mater" even

"factored into the selection process." Pet. App. 59 (emphasis added). The court of appeals agreed. Those schools "graduate[] thousands of students each year"; relatively few institutions had the required track records in this area; and it made no sense to disqualify some based on nothing more than where counsel got their degrees. Pet. App. 19.

Petitioners do no better in complaining that, because Google had donated money to other *cy pres* recipients, the payments were "changes to accounting entries" that "simply redirect[ed] money that the defendant would have given" anyway. Pet. Br. 32-33. Petitioners conceded below that the *cy pres* recipients would use the awards to fund new programs, not existing ones. See J.A. 164. Recipients "explained how the *cy pres* funds were distinct from Google's general donations." Pet. App. 16-17. Several recipients had challenged Google's practices, prompting lawsuits and government investigations. Pet. App. 16 n.7. Google, moreover, had previously "donated to hundreds of third-party organizations whose work implicates technology and Internet policy issues"; disqualifying them would have prioritized "less relevant or less qualified" organizations over "the interests of the class." Pet. App. 16, 18.

This Court "does not grant certiorari to review evidence and discuss specific facts." *United States* v. *Johnston*, 268 U.S. 220, 227 (1925). The courts below both carefully considered petitioners' contentions. Both applied the proper standard. And both properly found petitioners' contentions wanting.[13]

---

[13] Any challenge to attorney's fees—governed by Rule 23(h)'s reasonableness standard—is not properly before the Court. See pp. 40-41, *supra*. Nor was there an abuse of discretion. The district court

V. The Government's Jurisdictional Argument Counsels Dismissing The Petition As Improvidently Granted

The government argues that there is a "substantial" and "logically antecedent" question about whether any class members have suffered injury in fact so as to establish standing under *Spokeo, Inc.* v. *Robins*, 136 S. Ct. 1540 (2016). U.S. Br. 13-15. Neither court below addressed that contention. Nor did petitioners' opening brief. Ordinarily, "'this is a court of final review and not first view.'" *Adarand Constructors, Inc.* v. *Mineta*, 534 U.S. 103, 110 (2001) (per curiam). The existence of a previously unaddressed jurisdictional issue counsels dismissing the writ as improvidently granted. See, *e.g.*, *Izumi Seimitsu Kogyo Kabushiki Kaisha* v. *U.S. Philips Corp.*, 510 U.S. 27, 28 (1993) (per curiam); *Adarand*, 534 U.S. at 105.

That result is particularly appropriate here. This case is plagued with vehicle issues. Petitioners' primary arguments often lack relevance to this case. There was no "selling out" the class, as the settlement amounts are concededly adequate. See p. 16, *supra*. The question presented asks whether a settlement that "provides no

---

found the award appropriate, as the settlement was not "easily secured," coming only after class counsel defended against "three motions to dismiss" and "extensive in-person negotiations." Pet. App. 54-58. The court had ample discretion to adjust the award based on the circumstances. See *Fischel* v. *Equitable Life Assurance Soc'y of U.S.*, 307 F.3d 997, 1006-1007 (9th Cir. 2002). The outcome was in line with similar cases, 10 Wright & Miller, *supra*, § 2675.3 (awards typically 20-30%), and supported by class counsel's hours and rates, Pet. App. 55-57. There are few "sphere[s] of judicial decisionmaking in which appellate micromanagement has less to recommend it" than attorney's fees. *Fox* v. *Vice*, 563 U.S. 826, 838 (2011).

direct relief to class members" can satisfy Rule 23, Pet. i, but the settlement here does provide direct, prospective relief that addresses class members' injuries, see p. 13, *supra*. Many arguments (*e.g.*, the First Amendment and attorney's fees) are waived. See pp. 37, 40, *supra*. And Congress is currently considering legislation that addresses many of petitioners' purported concerns. See p. 10, *supra*. Not even the government suggests this Court address *Spokeo*'s application in the first instance here. The interests of decisional integrity compel dismissal.[14]

Under *Spokeo*, the "bare procedural violation" of a statutory right is not sufficient to confer Article III standing; instead, a "concrete injury" is required. 136 S. Ct. at 1549-1550. But a wide range of "intangible" harms may be sufficiently concrete given (a) their "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" and (b) Congress's judgment that the harm should be remedied. *Id.* at 1549; see *id.* at 1551 (Thomas, J., concurring) (noting that standing requirements are more lenient for private-party disputes).

Those considerations establish standing here. In a "great many of the cases" traditionally heard in Anglo-American courts—libel, false light, or privacy invasion—"the only harm is * * * to the plaintiff's dignity." 2 D.

---

[14] The government's proposal of remand (Br. 15) is unwarranted. The government regularly advises that certiorari should be denied where it has doubts about the plaintiffs' standing. See, *e.g.*, Gov't Br. in Opp. 9, *Flock* v. *Dep't of Transp.*, 137 S. Ct. 2268 (2017) (No. 16-1151); Gov't Br. in Opp. 16, *Stop Reckless Instability Caused by Democrats* v. *FEC*, 137 S. Ct. 374 (2016) (No. 16-109); Gov't Br. in Opp. 8, *Kent Recycling Servs., LLC* v. *U.S. Army Corps of Eng'rs*, 136 S. Ct. 2427 (2016) (No. 14-493). The equivalent is warranted here.

Dobbs, *Law of Remedies* §7.1(1), at 259 (2d ed. 1993); see also W. Page Keeton et al., *Prosser and Keeton on Torts* §117, at 851 (5th ed. 1984) ("the rights to privacy are recognized in virtually all jurisdictions"). Such "privacy" cases are actionable in federal court. *Time, Inc.* v. *Hill*, 385 U.S. 374, 384 & n.9 (1967). The Court's Fourth Amendment cases recognize that privacy is a cognizable interest capable of legal protection, even if its invasion may cause no pecuniary losses. See, *e.g.*, *Carpenter* v. *United States*, 138 S. Ct. 2206, 2213 (2018); *Arizona* v. *Hicks*, 480 U.S. 321, 326 (1987) (Fourth Amendment violated by officer lifting receiver to see serial number). There is no principled basis for rejecting Congress's determination that improper invasion of citizens' stored electronic information—unconsented circulation of their searches—should be actionable as well. See 18 U.S.C. §2702(a)(1)-(2). To the extent the Court chooses to address this previously unaddressed issue, standing should be upheld.

CONCLUSION

The decision below should be affirmed. Alternatively, the Court should dismiss the writ of certiorari as improvidently granted.

Respectfully submitted.

KASSRA P. NASSIRI
Counsel of Record
NASSIRI & JUNG LLP
47 Kearny St.
Suite 700
San Francisco, CA 94108
(415) 762-3100
kass@njfirm.com

MICHAEL ASCHENBRENER
KAMBERLAW, LLC
201 Milwaukee St.
Suite 200
Denver, CO 80206
(303) 222-0281
masch@kamberlaw.com

JEFFREY A. LAMKEN
MICHAEL G. PATTILLO, JR.
JAMES A. BARTA
WILLIAM J. COOPER
MOLOLAMKEN LLP
The Watergate, Suite 660
600 New Hampshire Ave., N.W.
Washington, D.C. 20037
(202) 556-2000
jlamken@mololamken.com

JUSTIN B. WEINER
JORDAN A. RICE
MOLOLAMKEN LLP
300 N. LaSalle St.
Chicago, IL 60654
(312) 450-6700

Counsel for Class Respondents

AUGUST 2018

APPENDIX

APPENDIX A

Federal Rule of Civil Procedure 23 (effective Dec. 1, 2009) provides as follows:

Rule 23. Class Actions

(a) PREREQUISITES. One or more members of a class may sue or be sued as representative parties on behalf of all members only if:

(1) the class is so numerous that joinder of all members is impracticable;

(2) there are questions of law or fact common to the class;

(3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and

(4) the representative parties will fairly and adequately protect the interests of the class.

(b) TYPES OF CLASS ACTIONS. A class action may be maintained if Rule 23(a) is satisfied and if:

(1) prosecuting separate actions by or against individual class members would create a risk of:

(A) inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class; or

(B) adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests;

(2) the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole; or

(3) the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy. The matters pertinent to these findings include:

(A) the class members' interests in individually controlling the prosecution or defense of separate actions;

(B) the extent and nature of any litigation concerning the controversy already begun by or against class members;

(C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and

(D) the likely difficulties in managing a class action.

(c) CERTIFICATION ORDER; NOTICE TO CLASS MEMBERS; JUDGMENT; ISSUES CLASSES; SUBCLASSES.

(1) *Certification Order.*

(A) *Time to Issue.* At an early practicable time after a person sues or is sued as a class representative, the court must determine by order whether to certify the action as a class action.

(B) *Defining the Class; Appointing Class Counsel.* An order that certifies a class action must define the class and the class claims, issues,

or defenses, and must appoint class counsel under Rule 23(g).

(C) *Altering or Amending the Order.* An order that grants or denies class certification may be altered or amended before final judgment.

(2) *Notice.*

(A) *For (b)(1) or (b)(2) Classes.* For any class certified under Rule 23(b)(1) or (b)(2), the court may direct appropriate notice to the class.

(B) *For (b)(3) Classes.* For any class certified under Rule 23(b)(3), the court must direct to class members the best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort. The notice must clearly and concisely state in plain, easily understood language:

(i) the nature of the action;

(ii) the definition of the class certified;

(iii) the class claims, issues, or defenses;

(iv) that a class member may enter an appearance through an attorney if the member so desires;

(v) that the court will exclude from the class any member who requests exclusion;

(vi) the time and manner for requesting exclusion; and

(vii) the binding effect of a class judgment on members under Rule 23(c)(3).

(3) *Judgment.* Whether or not favorable to the class, the judgment in a class action must:

(A) for any class certified under Rule 23(b)(1) or (b)(2), include and describe those whom the court finds to be class members; and

(B) for any class certified under Rule 23(b)(3), include and specify or describe those to whom the Rule 23(c)(2) notice was directed, who have not requested exclusion, and whom the court finds to be class members.

(4) *Particular Issues.* When appropriate, an action may be brought or maintained as a class action with respect to particular issues.

(5) *Subclasses.* When appropriate, a class may be divided into subclasses that are each treated as a class under this rule.

(d) CONDUCTING THE ACTION.

(1) *In General.* In conducting an action under this rule, the court may issue orders that:

(A) determine the course of proceedings or prescribe measures to prevent undue repetition or complication in presenting evidence or argument;

(B) require—to protect class members and fairly conduct the action—giving appropriate notice to some or all class members of:

(i) any step in the action;

(ii) the proposed extent of the judgment; or

(iii) the members' opportunity to signify whether they consider the representation fair and adequate, to intervene and present claims or defenses, or to otherwise come into the action;

(C) impose conditions on the representative parties or on intervenors;

(D) require that the pleadings be amended to eliminate allegations about representation of absent persons and that the action proceed accordingly; or

(E) deal with similar procedural matters.

(2) *Combining and Amending Orders.* An order under Rule 23(d)(1) may be altered or amended from time to time and may be combined with an order under Rule 16.

(e) SETTLEMENT, VOLUNTARY DISMISSAL, OR COMPROMISE. The claims, issues, or defenses of a certified class may be settled, voluntarily dismissed, or compromised only with the court's approval. The following procedures apply to a proposed settlement, voluntary dismissal, or compromise:

(1) The court must direct notice in a reasonable manner to all class members who would be bound by the proposal.

(2) If the proposal would bind class members, the court may approve it only after a hearing and on finding that it is fair, reasonable, and adequate.

(3) The parties seeking approval must file a statement identifying any agreement made in connection with the proposal.

(4) If the class action was previously certified under Rule 23(b)(3), the court may refuse to approve a settlement unless it affords a new opportunity to request exclusion to individual class members who had an earlier opportunity to request exclusion but did not do so.

(5) Any class member may object to the proposal if it requires court approval under this subdivision (e);

the objection may be withdrawn only with the court's approval.

(f) APPEALS. A court of appeals may permit an appeal from an order granting or denying class-action certifycation under this rule if a petition for permission to appeal is filed with the circuit clerk within 14 days after the order is entered. An appeal does not stay proceedings in the district court unless the district judge or the court of appeals so orders.

(g) CLASS COUNSEL.

(1) *Appointing Class Counsel.* Unless a statute provides otherwise, a court that certifies a class must appoint class counsel. In appointing class counsel, the court:

(A) must consider:

(i) the work counsel has done in identifying or investigating potential claims in the action;

(ii) counsel's experience in handling class actions, other complex litigation, and the types of claims asserted in the action;

(iii) counsel's knowledge of the applicable law; and

(iv) the resources that counsel will commit to representing the class;

(B) may consider any other matter pertinent to counsel's ability to fairly and adequately represent the interests of the class;

(C) may order potential class counsel to provide information on any subject pertinent to the appointment and to propose terms for attorney's fees and nontaxable costs;

(D) may include in the appointing order provisions about the award of attorney's fees or nontaxable costs under Rule 23(h); and

(E) may make further orders in connection with the appointment.

(2) *Standard for Appointing Class Counsel.* When one applicant seeks appointment as class counsel, the court may appoint that applicant only if the applicant is adequate under Rule 23(g)(1) and (4). If more than one adequate applicant seeks appointment, the court must appoint the applicant best able to represent the interests of the class.

(3) *Interim Counsel.* The court may designate interim counsel to act on behalf of a putative class before determining whether to certify the action as a class action.

(4) *Duty of Class Counsel.* Class counsel must fairly and adequately represent the interests of the class.

(h) ATTORNEY'S FEES AND NONTAXABLE COSTS. In a certified class action, the court may award reasonable attorney's fees and nontaxable costs that are authorized by law or by the parties' agreement. The following procedures apply:

(1) A claim for an award must be made by motion under Rule 54(d)(2), subject to the provisions of this subdivision (h), at a time the court sets. Notice of the motion must be served on all parties and, for motions by class counsel, directed to class members in a reasonable manner.

(2) A class member, or a party from whom payment is sought, may object to the motion.

(3) The court may hold a hearing and must find the facts and state its legal conclusions under Rule 52(a).

(4) The court may refer issues related to the amount of the award to a special master or a magistrate judge, as provided in Rule 54(d)(2)(D).

(As amended Feb. 28, 1966, eff. July 1, 1966; Mar. 2, 1987, eff. Aug. 1, 1987; Apr. 24, 1998, eff. Dec. 1, 1998; Mar. 27, 2003, eff. Dec. 1, 2003; Apr. 30, 2007, eff. Dec. 1, 2007; Mar. 26, 2009, eff. Dec. 1, 2009.)

APPENDIX B

Protecting Online Privacy: A National Initiative

A Proposal from AARP Foundation

As internet use continues to soar and as more and more daily transactions and interactions for both business and personal reasons are migrated online—it is a national imperative that people of all ages fully understand how to protect their privacy online. Just as reading, writing and arithmetic are critical requirements in life—so too now are the knowledge, skills and abilities to safely and effectively maintain an online presence. For these reasons, AARP Foundation proposes to develop a national initiative to educate and inform one million individuals over a three year period on how to protect their online privacy and proactively avoid the harmful impact of internet fraud and identify theft.

As the charitable arm of AARP, AARP Foundation is dedicated to creating solutions that help vulnerable Americans secure the essentials and maintain their independence. AARP is the leading, national expert on people 50+, with access to data and research regarding each socio-economic segment of the population. AARP Foundation works closely with the larger AARP enterprise to understand the needs of vulnerable older adults, their families, and their communities, and works to identify, implement and bring to national scale interventions to meet those needs. With a presence in all 50 states and multiple channels for delivering timely, relevant and actionable information, we are well-positioned to reach individuals of all ages and deliver important content on online privacy protection.

AARP Foundation is uniquely qualified to administer this program and develop, implement, scale and sustain

consumer facing tools and services designed to help individuals protect their online privacy and manage their flow of data. While AARP and AARP Foundation's overall focus is on older adults—we are a trusted brand to people of all ages. AARP Foundation has an exemplary record of providing service and consumer education on a wide variety of topics and has the requisite communication channels, national and local partnerships, research capability, infrastructure, human capital, and transparent reporting mechanisms to transform how consumer facing education and information on online privacy is delivered and measured. Last year alone, AARP Foundation served over 3.2 million individuals across its programmatic efforts.

AARP Foundation's consumer protection programs have arguably been subjected to more scientific scrutiny than any consumer protection program in the country. No fewer than four major studies have been done to measure the behavior change effects of our peer counseling model. In each case, the program has shown that recipients of the services retain the information they receive, resist subsequent malicious attempts that occur after receiving counseling, retain the information over a prolonged period of time, and are more knowledgeable in general about how to protect themselves.

After a careful internal review, we have determined that accepting cy pres funding for this effort would not pose a conflict of interest for either AARP or AARP Foundation as neither entity receives funding from nor is in partnership with Google. Both organizations are free and independent from any relationship with Google or its employees.

Initiative Goals and Objectives

To implement this wide-scale, national effort, we will employ a number of different strategies to ensure we are reaching a diverse range of consumers with relevant, timely, actionable, and credible information, tools and resources to develop the skills and knowledge to protect their online privacy. These different methods will be designed specifically to meet the intent of the settlement and will include:

1. **Expanding AARP Foundation's existing and multi-tiered regional consumer protection call center operations.**

AARP Foundation currently operates three regional call centers that employ highly trained volunteers to respond to in-bound calls from consumers and conduct proactive outbound calling to educate those at risk on issues related to fraud and how to protect their privacy. Research conducted by AARP Foundation and the Department of Justice showed the high correlation between peer assistance and individuals taking the necessary steps to protect themselves from fraud. Our volunteers go through intensive training from the initial 25 hours of curriculum and on-the-job training provided by staff through to ongoing education on at least a quarterly basis conducted by experts from the SEC, Attorney Generals' Offices, the FBI, Legal Aid services and many more. For this effort, we would develop specific training for volunteers on the latest information and best practices for online privacy protection.

2. **Develop a communications campaign including enhancing current website with online privacy focused content**

To reach even more people with information and resources, AARP Foundation will develop a communica-

tions campaign and enhance its website with focused content on online privacy protection and will develop a unique and engaging consumer-facing tool for individuals to assess their current practices related to sharing private information and specific actions to take to increase their protection and better manage their flow of data for all aspects of online interactions and transactions including social media, banking, website navigation, etc. This enhanced website will be an unparalleled national and open-source resource for individuals wanting the latest information on privacy protection and will be a repository for content, tools and resources available to consumers and intermediaries.

3. Build local consumer protection programs, events and sustained capacity

AARP Foundation will utilize a portion of the funding to build the capacity of national, state and local organizations and AARP state offices to provide consumer education programs related to online privacy protection. This capacity building effort will include developing curriculum and "train-the-trainer" toolkits and materials for local education activities and providing capacity building and planning grants to key organizations to sustain the program past the period of the funding. Specific consumer education and training materials will be developed and disseminated through workshops and events coordinated with the AARP state offices and national, state and local partners to consumers and staff and volunteers of key organizations supporting this effort.

4. Build unprecedented research and data on online privacy protection

A critical component of this effort will be adapting AARP Foundation's existing database management system to create an "early warning system" that tracks

trends and threats to online privacy. This data can then be shared with staff, volunteers, law enforcement, policy makers, and consumers to enable them to take action to increase privacy protection efforts. This database will be one of the largest collections of threats to privacy and consumer fraud trends in the country and will give AARP Foundation and its partners the ability to know how to target education and outreach efforts on a real-time basis.

Transparency in Publishing Results and Outcomes

AARP Foundation has implemented an organization-wide process for evaluating all projects, grants and programs. We also promote transparency by publishing the results of our programs, grants and initiatives on our website and via our annual reports. At any given time, consumers, funders and other stakeholders can see the results and impact of our efforts. This process includes developing a Logic Model that evaluates and measures the social change that occurs as a result of our efforts. As part of the development of the logic model for this project, we have initially identified the following social impact outcomes and the related metrics we will track to ensure we are meeting these outcomes:

There is increased awareness of online privacy protection efforts	• At least 1 million people served over the three year funding period. (Quantitative)
Increase in the number of individuals who take steps to protect their private information and manage their flow of data	• Number of people contacted or attending events who take action to protect online privacy. Baseline to be es-

	tablished in Year 1 of funding and increase measured in Years 2 and 3 (Quantitative) • Feedback and stories from consumers. (Qualitative)
There is increased capacity of local communities and organizations to support online privacy protection efforts.	• Number of partners engaged. (Quantitative) • Number of community education and "train the trainer" events held. (Quantitative)

Infrastructure and Partners

To minimize infrastructure costs and maximize funding for programmatic work, call center operations will be operated out of existing AARP Foundation regional call centers in Seattle, Washington and Denver, Colorado, and Charleston, West Virginia. These call centers have a successful track record for reaching consumers, and have expert staff and trained volunteers ready to conduct outreach minimizing ramp up time for the program.

In addition, AARP Foundation will leverage AARP State Offices located in every state to implement state and community-based outreach efforts, events and workshops that help build capacity to respond to specific issues related to online privacy protection and online fraud.

As part of this effort, AARP Foundation will continue to work closely with the Federal Trade Commission, state attorneys general, the FBI, the Financial Industry Regulating Authority (FINRA), the State Dept. of Financial Institutions, the Centers for Medicare and Medicaid Services (regarding Medicare fraud), and local law

enforcement agencies to build expertise on online privacy protection.

Organizational Capacity

AARP Foundation works across the country with existing and results-driven organizations at the local and state level, coordinating responses to address issues facing low-income older adults to most effectively reach people in ways relevant to their needs and their community. This approach maximizes the impact of our resources, reinforces and builds solutions from the ground up, avoids duplication of effort, and creates a powerful multiplier effect for change.

AARP Foundation has proven capacity and capability to manage a project the size and scope of this project as evidenced by our highly effective Tax-Aide and long history of operating consumer fraud prevention programs. In 2013, Tax-Aide deployed 35,000 volunteers in 6,000 locations across the country to provide free tax preparation services for 2.6 million people.

Consumer protection has been core to AARP Foundation's work for many years. In 2005, a settlement between a multi-state group of attorneys general and Western Union resulted in a multi-million dollar charitable contribution to the AARP Foundation to fight fraud. A second settlement between the states and Moneygram in 2008 resulted in an additional $1.1 million contribution to the AARP Foundation. Most of the funding from these settlements went to the creation and operation of eight regional Fraud Fighter Call Centers and community-based programs that used evidenced-based techniques to fight elder financial abuse.

Currently, AARP Foundation operates ElderWatch and Fraud Prevention programs around the country.

These programs work in communities to provide education about scams and frauds through public outreach events, media, website exposure, mailings, etc. Central to the fraud fighting efforts, however, are inbound and outbound call centers staffed by trained volunteers. The inbound call centers offer assistance in filing complaints with the state's Attorney General, mediation services, client/company intervention, referrals, education and assistance. Based on research conducted between AARP Foundation and the Department of Justice showing the high correlation between peer assistance and behavior change related to avoiding fraud, the outbound call centers provide peer-to-peer education to consumers all across the country, informing them about current frauds and scams and providing assistance with navigating the complaint process, as applicable. In 2012 alone through these call center operations, AARP Foundation had direct contact with over 200,000 consumers.

For its consumer protection work, AARP Foundation has a strong track record that has attracted multiple funders. In addition to the Colorado, Washington state, and West Virginia Attorney General's offices, additional funders of our work include FINRA Foundation, the Washington State Insurance Commissioner, the Administration on Aging (AoA) and the Charles Schwab Foundation.

Project Management and Staffing

AARP Foundation's experienced management team is committed to the success of this project.

Emily Allen is the Vice President, Income Impact with AARP Foundation and will serve as the lead for the program and provide strategic direction and oversight. Throughout her career, Ms. Allen's primary passion has been on serving the needs of those most at

risk in our communities. She has served in a number of capacities in the non-profit, education and asset building arenas and has worked across the generations to ensure vulnerable and at risk individuals have access to the resources and services they need to thrive. Currently, Ms. Allen is responsible for the development of strategies and interventions to ensure that low income older adults increase their economic stability obtaining quality jobs in their communities and by increasing their access to appropriate and affordable financial products and services. Ms. Allen holds a Bachelor's Degree in Psychology from Westminster College and a Master's Degree in Human and Organizational Learning from The George Washington University.

Amy Nofziger, Director – Regional Operations, AARP Foundation. Amy has worked at AARP Foundation's ElderWatch program since its inception in 2001, first as the Program Coordinator and then as the Program Leader. More recently Amy took on the responsibility as the Director of Regional Operations for the AARP Foundation Income Impact area. She is responsible for regional program management and operations for the Income program areas.

Amy serves on the Colorado Nonprofit Association Leadership Advisory Committee. She was appointed to the State of Colorado's Elder Abuse Task Force and sits on the Public Guardian Advisory Committee. Previously, Amy was the chairwoman of the advisory board for the Colorado Coalition for Elder Rights and Abuse Prevention (CCERAP). She has presented to over 75,000 seniors and professionals on consumer fraud, workforce initiatives and other social issues facing older adults. Amy has a degree in criminology/sociology from Ohio Univer-

sity, a certificate in gerontology from the University of Denver, and is a trained mediator.

Doug Shadel, PhD, AARP Washington State Director – Project Advisor. Shadel is one of the leading experts in the United States on financial exploitation of older persons. He is a former fraud investigator who has co-authored numerous books on the topic including *Schemes & Scams*, *Weapons of Fraud* and *Outsmarting the Scam Artists*. He has also co-authored numerous studies on fraud and has been invited to present at the National Academy of Sciences, the U.S. Securities and Exchange Commission, the Federal Trade Commission and to the U.K.'s Fair Trading Bureau in London. Shadel recently presented research findings to an internet fraud summit in Germany cosponsored by Microsoft and a number of European authorities. Shadel holds a bachelor's degree in political science, a master's in public administration and a PhD in social science.

Budget

Personnel	.5 FTE Salary and Benefits - 50K/year for 3 years	$150,000
Web and Technology	Upgrades and customization for existing Foundation Website and Impact System - 50K fixed cost, 25K/year for 2 years	$100,000

Regional Call Center Operations	Volunteer expenses, operational costs - 100K/year for 3 years	$300,000
Contracts	Curriculum development (25K fixed cost); evaluation (50K fixed cost)	$75,000
Grants	Capacity building grants for program sustainability to 4 regional organizations 50K/organization in year 3.	$200,000
Total Direct Costs		$825,000
Indirect Costs	10% Indirect Cost Rate (ICR)	$82,500

APPENDIX C

[Berkman Center for Internet & Society at Harvard University logo omitted on each page of Appendix C]

Search for Privacy:

Blueprint for Better Protection of Search Engine Users and Their Data

Executive Summary

The Berkman Center for Internet & Society at Harvard University is a university-wide, interdisciplinary program founded to explore cyberspace, share in its study, and help pioneer its development. Since its inception in 1997, the Center has engaged in extensive research, educational, and other relevant activities on cutting edge issues related to the Internet. Research, teaching, and engagement around risks to privacy and reputation in the digital age—as well as new approaches to protect it—are integral to the Berkman Center's mission.

Among the most frequently used services on the Internet are search engines, which have developed over the years from relatively simple tools to locate information to highly sophisticated and commercially immensely profitable services that are an important part of today's Internet economy. Search engines are not only indispensable navigation aids in the digital age. They also pose a significant risk to consumer privacy by accumulating an unprecedented amount of data about almost everything we search for and click on the Internet. A series of recent privacy cases and incidents where users search data has been shared with third parties without their knowledge or consent illustrates the problem where adequate privacy safeguards fail or do not exist.

To work towards a solution, the Berkman Center proposes an initiative to develop concrete proposals for safe-

guarding Internet privacy more effectively via legal and policy reform, company action, technological innovation, targeted education and user outreach. Bringing together like-minded individuals and organizations that share our mission to strengthen user privacy, we will develop a blueprint that demonstrates how users of search engines can be better protected in the future. Based on a thorough, independent analysis of search-relevant privacy cases and incidents, we will evaluate to what extent existing legal and regulatory frameworks succeed or fail in protecting consumer privacy, and how we can close gaps by adding new privacy safeguards. Outputs of the proposed initiative include specific recommendations targeted at lawmakers and relevant companies, as well as materials, resources, and tools that enable users to make informed choices about their data—and better control it—when searching the Internet.

The initiative will draw together a community of users, practitioners, company representatives, advocates, and technologists who want to take action on Internet privacy by influencing company behavior, strategically educating policymakers, and empowering users.

Proposed Initiative

Problem Statement and Objectives

The litigation and settlement in re Google Referrer Header Privacy Litigation exemplifies a growing number of instances where business practices by Internet companies threaten the privacy of their users. This case and similar incidents demonstrates a lack of adequate safeguards to protect privacy online and mitigate the associated risks for consumers. While business and revenue models, rapid technological innovation, and the behavior of users are important factors that shape privacy risks online, the litigation also suggests that existing legal and

policy frameworks aimed at protecting privacy have not adequately kept up with changing data collection, processing, and sharing practices. Especially in the highly interconnected "big data" environment that defines cyberspace today, these systems are not adequately protecting everyday users.

With a focus on the changing landscape of online search, and leveraging many years of privacy research, teaching, and policy work, the Berkman Center proposes a research-based multi-stakeholder law and policy initiative aimed at formulating concrete proposals for how Internet privacy can be safeguarded more effectively, via legal and policy reform, company action, technological innovation, targeted education and outreach. Analyzing recent privacy cases and incidents—starting with the litigation at hand—and considering emerging and soon-to-be emerging technological developments (e.g. Google Glass, sensor networks, the Internet of Things), as well as advancements in the data analysis capabilities that underlie online searching, the proposed initiative will:

1. Catalog and analyze current and future privacy threats resulting from search technology and corresponding business practices, beginning with in-depth comparative analysis of relevant cases and examples;
2. Examine and investigate existing legal and regulatory frameworks and critically evaluate to what extent current legal instruments and doctrines are suitable or fail to effectively and efficiently protect consumer privacy in the evolving online search ecosystem;
3. Develop, in partnership with relevant stakeholders, a set of scenarios, at the intersection of law, technology, and business practices that outline concrete ways to improve user privacy online, with a focus on search; and,

4. Share these findings in creative formats with relevant stakeholders and target audiences, with the goal of raising awareness regarding privacy risks and potential alternatives or remedies.

   →The ultimate ambition of the proposed initiative is to develop a blueprint that demonstrates how users who are engaged in online search can be better protected in the future; based on the blueprint, we will generate a set of specific recommendations targeted at lawmakers and regulators, as well as relevant companies.

While these specific outcomes are central to the initiative, arguably just as important is the process of building a collaborative network, where essential knowledge can be transferred between relevant actors, and findings can be transformed into concrete actions. As the Berkman Center takes the lead in developing the blueprint and is responsible for recommendations and other key outcomes, the initiative will simultaneously engage a diverse set of stakeholders who play a role in the evolving online search ecosystem, including search technology users, consumer watchdogs and privacy organizations, search technology developers, search providers, advertisers, and regulators. Such multi-stakeholder processes have informed previous policy-oriented initiatives by the Berkman Center and increased the impact of their outcomes. For instance, our work on digital media and copyright, interoperability, freedom of speech, cloud computing regulation, and many other topics have been shaped by extensive consultation and collaboration with a broad set of stakeholders.

This type of initiative is central to the Berkman Center's mission: to investigate the real and possible boundaries in cyberspace between open and closed systems of code, of commerce, of governance, and of education, and

the relationship of law to each. We do this through active rather than passive research, believing that the best way to understand cyberspace is to actually build out into it. Our research and allied work all shares a commitment to advancing the public interest, and holding legal and policy frameworks accountable to that same standard.

The proposed initiative—to explore ways to preserve consumer privacy in a rapidly expanding online ecosystem in which search plays such an important role—will build directly upon previous Berkman research activities and advocacy work on online privacy, as further described below. The initiative will also benefit from important connection points with a series of ongoing projects, including our continuing work on information and communications technology (ICT) interoperability. Important insights regarding the interplay of legal instruments and privacy-protecting mechanisms in computer science, such as differential privacy, can be transferred from our National Science Foundation project on Privacy Tools for Sharing Research Data. Our series of influential youth privacy reports will provide a foundational understanding of how youth behave and seek information online, with a special focus on deepening our understanding of how youth understand privacy risks. In addition to our rich community of faculty, fellows and staff, we will also engage experts from our growing network of collaborators via our global network of interdisciplinary Internet & Society research centers, where comparative perspectives on privacy issues are also center stage.

Workplan, Timeline, and Methodology

Activities under the proposed initiative can be divided into five analytically distinct, but interrelated phases with different methodologies at work.

Phase 1	Information gathering: Understanding the online search ecosystem and related privacy risks

Activity: During the initial phase, we will carry out a comprehensive review and synthesis of the online search ecosystem and its key constituencies, including applicable privacy policies and practices, developments in search technology, evolving business practices, and relevant trends in user behavior, all with the goal of identifying current and future privacy threats as well as opportunities for possible interventions. As part of this process, we will aim to understand how one group of consumers, youth, conceives of and responds to issues of data privacy.

Methods: We will employ various methodologies, including development of use cases and case studies, a review of search-related privacy incidents, a literature review, expert and selected focus group interviews with users, and the formation of a multi-stakeholder working group which will convene for a series of meetings.

Timeline: 6 months.

Milestones: Multi-stakeholder working group launch meeting, project website.

Phase 2	Analysis and evaluation: Mapping the relevant legal and policy landscape

Activity: Based on findings from phase 1, the Berkman team will create a typology and corresponding "heatmap" of search-related privacy challenges and issues for consideration. This will serve as the basis for an in-depth analysis of the relevant legal and regulatory frameworks, broadly defined, with the goal of evaluating the current "state of play" with respect to the levels of privacy protection of users of online search technology. The evaluation will be based on a "scorecard" system, *i.e.* a set of criteria, developed in collaboration with stakeholders, which will enable continued assessment of legal and regulatory frameworks over time and measure success. This mapping will also explore gaps in knowledge or understanding, with the goal of identifying specific areas for education or intervention.

Methods: The team will engage in qualitative research, including traditional legal research and doctrinal analysis as well as economic analysis; it will also apply techniques borrowed from emerging regulatory issues analysis and horizon scanning.

Timeline: 6 months.

Milestones: Interactive heatmap, "scorecard," interim report.

Phase 3	Consultation: Engaging and consulting relevant stakeholders and soliciting feedback on anticipated outputs and work to date

Activity: The insights and findings from these initial activities will be shared through a series of multi-stakeholder working meetings. These gatherings will also provide an opportunity to develop a collective understanding of both the problem and the potential solution space for privacy challenges related to online search. A particular emphasis will be on the identification of scenarios and targeted interventions that could improve the status quo and increase the levels of privacy protection for users of online search technology. A focus will be on legal and regulatory interventions, including enforcement issues, in addition to areas for user education and enhanced understanding of privacy risks (and possible alternatives).

Methods: Multi-stakeholder working meetings, expert interviews, and—possibly—a small number of commissioned papers, including a comparative law analysis.

Timeline: 3 months.

Milestones: Working meetings, potential analytical pieces based on takeaways from working meetings.

Phase 4	Synthesis

Activity: In the fourth phase, the Berkman team will synthesize the work from the previous activities and work towards a blueprint that outlines how the privacy of users who are engaged in online search can be better protected in the future. Based on the blueprint, the team will generate a set of specific recommendations targeted at lawmakers and regulators, in addition to relevant ICT

companies. It will also seek to explore or envision opportunities to enhance user understanding of risk, with the goal of developing tools or other educational materials that can be used by users (and perhaps forward-leaning companies). The draft blueprint and the recommendations will be shared with the multi-stakeholder group and outside experts, including privacy advocacy groups.

Methods: Qualitative analysis.

Timeline: 6 months.

Milestones: Blueprint and recommendations.

Phase 5	Outreach and public communications of findings

Activity: While outreach will occur in parallel to the four phases outlined above, the proposed initiative would conclude with a strategic effort to engage in knowledge transfer and the targeted sharing of the blueprint and recommendations with lawmakers and regulators and the public at large.

Methods: Outreach event in Washington D.C.; policy briefings with decision-makers; media calls, as appropriate.

Timeline: 3 months.

Milestone: D.C. event.

Target Group and Value Added

The target group of the initiative closely aligns with the Members of the Class, which according to the complaint are "all persons in the United States who submit-

ted a search query to Google at any time between October 25, 2006 and the date of notice to the class of certification." A more specific approximation of the demographics of the Class can be inferred from a 2012 report by the Pew Research Center, according to which 83% of searchers used Google as a search engine. The report found that search is particularly popular among young adult Internet users, users who have been to college, and those with the highest household incomes.

The targeted group of the proposed initiative aligns closely with the Class at three levels and across the different phases of the project, as outlined in the previous section:

- *Multi-stakeholder working group:* A select number of search engine users will be invited to participate in the multi-stakeholder working group and in the respective meetings. A focus will be on young adult users.
- *Consultation process:* The draft documents resulting from the proposed initiative will be shared over the project website with all class members, who are invited to provide feedback.
- *Blueprint and recommendations:* The proposed initiative is aimed at improving the level of privacy protection of users who use search technology online through changes in the legal and regulatory framework. By definition, this group includes all Class Members.

At the core of the case is the allegedly unlawful disclosure of the contents of search queries of Google users to third parties. The interest of the Class is in being protected against future privacy violations and non-transparent data-sharing by the search engines provider.

The proposed initiative responds to these issues by benefiting the Class directly and in at least three ways:

- *Knowledge base about threats*: The initiative seeks to inform Internet users about current and future privacy threats related to online searching, while offering a critical assessment of gaps and limitations of the current legal and regulatory framework, including enforcement regimes. Importantly, this assessment will include an analysis of user expectations and attitudes, with an eye towards creating educational materials that will better inform consumers and policy makers about the technologies they use (and regulate). This foundational analysis will not only educate the Class members on the privacy risks associated with online search, but also empower them to take deliberate and effective preventive measures as desired.
- *Policy blueprint and recommendations*: The initiative will result in a blueprint and associated recommendations for lawmakers and regulators aimed at increasing the future level of privacy protection for the users of online search technologies—including the class members. As such, it seeks to protect the Class from future wrongful conduct of which the plaintiffs complain.
- *Educational materials*: Finally, the Class will benefit from creative educational materials designed to respond to gaps in knowledge regarding privacy risks, and that are based on findings emerging from a collaborative, networked process with key actors in the field. These outputs will ideally complement ongoing efforts to raise awareness and help users and policymakers understand the more complex elements of search technologies, and therefore make informed choices about the products they use.

Deliverables, Reporting, and Evaluation

The objectives and deliverables have been described in the action plan and are both measurable and subject to evaluation.

Key deliverables include:

- Heatmap identifying and prioritizing search-related privacy risks
- Research outputs, including a series of papers and briefing materials
- Blueprint and recommendations addressed to lawmakers and regulators
- Creative educational and outreach materials, grounded in data on user concerns regarding search-related privacy risks

Each draft deliverable will be subject to a peer review, shared among the members of the multi-stakeholder working group, which includes search engine users, and will be part of an open consultation process, in which the Class can participate and provide feedback. All findings and outcomes will be made accessible over a project website on the Berkman Center's homepage.

The outcomes and effectiveness of the proposed initiative will be reported in one midterm and one final report, available to the Class and the public at large through a project website on the Berkman Center's homepage. The reports will be structured in a manner similar to the narrative portion of a grant report. Moreover, all findings and materials resulting from the initiative—including, for instance, the summaries of the multi-stakeholder working meetings as well as the typology of search-related privacy threats and challenges, in addition to educational materials—will be shared online and pre-

sented in a manner that is accessible to a broader audience, including the Class, policymakers and companies.

Team

The initiative will be staffed as follows: Professor Urs Gasser will serve as the Principal Investigator of the initiative, in close collaboration with the Berkman Center's incoming Faculty Chair and Co-Founder Professor Jonathan Zittrain. They will be supported by a part-time project manager as well as three research fellows and two research assistants. The Cyberlaw Clinic at the Berkman Center, led by managing director Chris Bavitz, will provide additional capacity and facilitate student participation in the project. The Berkman core team will provide support in areas such as financial administration, event management, and outreach/communications.

Urs Gasser

[photograph omitted]

Urs Gasser is the Executive Director of the Berkman Center for Internet & Society at Harvard University and a Professor of Practice at Harvard Law School. He is a visiting professor at the University of St. Gallen (Switzerland) and at KEIO University (Japan), and he teaches at Fudan University School of Management (China). Urs Gasser serves as a trustee on the board of the NEXA Center for Internet & Society at the University of Torino and on the board of the Research Center for Information Law at the University of St. Gallen, and is a member of the International Advisory Board of the Alexander von Humboldt Institute for Internet and Society in Berlin. He is a Fellow at the Gruter Institute for Law and Behavioral Research. Dr. Gasser has written and edited several books, and published over 100 articles in professional journals.

Jonathan Zittrain

[photograph omitted]

Jonathan Zittrain is Professor of Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, and co-founder of the Berkman Center for Internet & Society. His research interests include battles for control of digital property and content, cryptography, electronic privacy, the roles of intermediaries within Internet architecture, human computing, and the useful and unobtrusive deployment of technology in education. He performed the first large-scale tests of Internet filtering in China and Saudi Arabia, and as part of the OpenNet Initiative co-edited a series of studies of Internet filtering by national governments, including Access Denied: The Practice and Policy of Global Internet Filtering, and Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. He is a member of the Board of Trustees of the Internet Society, the Board of Directors of the Electronic Frontier Foundation, and the Board of Advisors for Scientific American. He has served as a Forum Fellow of the World Economic Forum, which named him a Young Global Leader, and Distinguished Scholar-in-Residence at the Federal Communications Commission. His book The Future of the Internet—And How to Stop It is available from Yale University Press and Penguin UK—and under a Creative Commons license. Papers may be found at http://www.jz.org.

Christopher Bavitz

[photograph omitted]

Christopher T. Bavitz is Managing Director of Harvard Law School's Cyberlaw Clinic, based at the Berk-

man Center for Internet & Society. He is also a Clinical Professor of Law at Harvard Law School, where he co-teaches the Practical Lawyering in Cyberspace seminar and teaches the seminar, Music & Digital Media. Chris concentrates his practice on intellectual property and media law, particularly in the areas of music, entertainment, and technology. He oversees many of the Clinic's projects relating to copyright, speech, and advising of startups, and he serves as the HLS liaison to Harvard's Innovation Lab. Prior to joining the Clinic, Chris served as Senior Director of Legal Affairs for EMI Music North America. From 1998-2002, Chris was a litigation associate at Sonnenschein Nath & Rosenthal and RubinBaum LLP/Rubin Baum Levin Constant & Friedman, where he focused on copyright and trademark matters. Chris received his B.A., cum laude, from Tufts University in 1995 and his J.D. from University of Michigan Law School in 1998.

Sandra Cortesi

[photograph omitted]

Sandra Cortesi is a Fellow at the Berkman Center and the Director of the Youth and Media project. She is responsible for coordinating the Youth and Media's policy, research, and educational initiatives. At the new Youth and Media Lab Sandra works closely with talented young people and lead researchers in the field as they look into innovative ways to approach social challenges in the digital world, including the production and exchange of digital media, youth development in social networking, and digital citizenship. Together with Urs Gasser and the YaM team, she focuses on the topics of "information quality" and privacy, about which she has coauthored several publications. Sandra also examines a broad range of youth communication and information technology prac-

tices for insights into youth online behavior and emergent policy questions, where she applies her training as a cognitive scientist. Sandra continues to also be engaged in international projects. Sandra has a Masters in Psychology, with a specialization in Neuro-Psychology and Human-Computer Interaction, from the University of Basel.

Paulina Haduong

[photograph omitted]

Paulina Haduong is a Master's Candidate in Technology, Innovation, and Education at the Harvard Graduate School of Education. She is interested in the intersection of education, technology, and art. She is a Co-Founder of the Sexual Literacy Forum at Yale and holds a BA in Linguistics from Yale University, where she was a member of Berkeley College.

Budget

The Berkman Center respectfully requests $935,000 in funding from this cy pres award. Budget for two years of activity is as follows:

Salary and Fellowship:	**$593,800**
Principal Investigator	$74,000
Co-Principal Investigator	$22,000
Clinical Instructor	$75,000
Research Fellows (2/year @ $48,000)	$192,000
Project Management, Outreach	$140,800
Research Assistants, Student Interns	$90,000

Fringe Benefits:	**$198,950**
Travel and Events:	**$75,500**
Working meetings (5, various cities)	$17,500
Focus groups (3, various cities)	$10,500
Policy briefing, DC	$7,500
Staff travel (meetings, conferences)	$20,000
Public outreach	$10,000
Other Project Expenses	**$66,750**
Editorial svcs, graphic design	$3,000
Computing resources	$10,000
Honoraria (5 papers @ $2,000)	$10,000
Subject payments	$2,500
Technical development	$40,000
Supplies, misc project expenses	$1,250
Total:	**$935,000**

Brief History of the Berkman Center

The Berkman Center for Internet & Society at Harvard University is a research program founded to explore cyberspace, share in its study, and help pioneer its development. Since 1997, the Center has been home to an ever-growing community of faculty, fellows, staff, and affiliates working on projects that span the broad range of intersections between cyberspace, technology, and society.

Our global community works collaboratively on cutting edge issues at the intersections of new technology and media including governance, innovation, privacy, intellectual property, cooperation, learning, youth, underserved communities, freedom of expression, and civic engagement.

Relevant Experience and Previous Activities (Selection)

Research, teaching, and engagement around the risks and opportunities related to privacy in a digital age are integral to the Berkman Center's mission and have informed our work in foundational ways. Our underlying approach to studying privacy has been to learn and share across projects and areas of inquiry, as well as with researchers in our extended network, including colleagues outside the U.S.

Research

The Berkman Center has long been home to a number of cross-disciplinary initiatives that investigate privacy and privacy-relevant questions in the digitally networked environment. We offer research, resources, workshops, and other outputs focused on key privacy issues, aiming to pinpoint novel solutions to privacy problems that reconcile technological, legal, political, economic, and behavioral tensions and maximize capacity for innovative and effective uses of data and communications. Our most recent work in the privacy space includes the Student Privacy Initiative, the Youth and Online Privacy Initiative, and the Privacy Tools for Sharing Research Data project. Each of our efforts builds upon engagement with and outreach to diverse stakeholders for whom privacy questions are particularly relevant, including educators, policy makers, industry representatives, advocates, and other scholars. This interdisciplinary, multi-stakeholder

model empowers our team to surface, identify, and analyze critical emerging questions and challenges, to support efforts to promote and preserve privacy rights, and to design and implement practical systems that allow research findings to benefit society.

- Since 2012, the Berkman Center's Youth and Media (YaM) team has been engaged in a Youth and Online Privacy initiative in partnership with the Pew Research Center focused on gaining a more nuanced understanding of youths' conceptions of privacy, how these conceptions may differ from adult perspectives, and how they are reflected in the kinds of activities in which youth engage online. As part of this project, the YaM team conducted focus group interviews with over 200 youth across the country, while Pew administered a nationally representative survey. Together five seminal reports on youth and privacy were co-authored and released, with "Teens, Social Media, and Privacy" as a flagship report. Across these and related efforts, the team has explored the following research questions, among others:
    - What concepts equivalent to "privacy" are embedded in how youth use social media?
    - What kinds of activities do youth engage in when they are online and how do they control the information they post on websites, and more specifically, on social media platforms?
    - Who do youth primarily interact with when they're online? How do youth view relationships with adults and with their peers online?
    - How do youth perceive and respond to Internet restrictions their schools and/or parents might have put in place?

- How do youth perceive and respond to online ads?
- How can we foster a grounded discussion about what technologies—and which associated policies—would be most useful and appropriate, particularly in the educational context?

- Moving forward, the Youth and Media team explores, as part of the Student Privacy Initiative described below, how new online platforms and tools can shape, improve, and expand students learning experiences while protecting their privacy.

Across formal and informal educational settings, increasingly powerful and innovative ICT products and services offer tremendous potential for schools to provide educators and students with new platforms and tools to shape, improve, and expand learning experiences, even in the face of continually shrinking budgets. However, these benefits are also accompanied by critical privacy questions and concerns, especially around the collection and use of student data. Beginning in early 2013, the Berkman Center's Student Privacy Initiative launched a multidisciplinary, multi-stakeholder conversation focused on how these privacy considerations intersect with existing policy regimes as well as with emerging developments in educational theory (e.g., connected learning) and institutional practices (e.g., refining technology policies within an individual school). Since launching, the Initiative has contributed to the student privacy and technology field with a number of timely publications and workshops, including the following: "Privacy and Children's Data: An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act;" "Student Privacy in the Cloud Computing Ecosystem: State of Play & Po-

tential Paths Forward;" "Youth Perspectives on Tech in Schools: From Mobile Devices to Restrictions and Monitoring;" "Student Privacy & Cloud Computing at the District Level: Next Steps and Key Issues;" and "K-12 Edtech Cloud Service Inventory," which drew from a November 2013 Berkman and Consortium for School Networking (CoSN) co-organized working meeting.

- Information technology, advances in statistical computing, and the deluge of data available through the Internet are transforming social science. However, a major challenge for researchers is maintaining the privacy of human subjects. Led collaboratively by Harvard University's Center for Research on Computation and Society (CRCS) at the School of Engineering and Applied Sciences, Institute for Quantitative Social Science (IQSS), and Berkman Center for Internet & Society, with support from the Secure and Trustworthy Cyberspace (SaTC) program at the National Science Foundation, the Privacy Tools for Sharing Research Data project seeks to develop methods, tools, and policies to bolster the tremendous value that can come from collecting, analyzing, and sharing data while more fully protecting individual privacy.

Education

The Berkman Center has a long-standing track record on educating students and the public at large on privacy issues. Early explorations on the topic during the 1990s and early 2000s include: privacy-focused sections in the first "Internet & Society" courses at Harvard Law School and in the Berkman Center's global iLaw seminars; and a "Privacy in Cyberspace" course offered in 1999-2003 through the "Berkman Online Lectures & Dis-

cussions" program, which also tackled consumer privacy in its E-Commerce offering. In 2006, the Berkman Center convened the Identity Mashup Conference as the culmination of a two-year effort to explore the role of identity systems in strengthening privacy, civil liberties and new forms of civic participation and commerce. More recent activities include the following:

- *Ongoing engagement with privacy-related issues* in courses such as Practical Lawyering in Cyberspace (Harvard Law School), Difficult Problems in Cyberspace (Harvard Law School-Stanford Law School joint course), Online Business and Law Seminar (Harvard Law School), Cyberspace in Court: Law of the Internet (Harvard College Freshman Seminar), Internet & Society: Technologies and Politics of Control (Harvard Extension School), and Comparative Online Privacy, a seminar led by Executive Director Urs Gasser in Spring 2014 (Harvard Law School).
- Privacy within business, non-profit, and research contexts has been a significant area of focus for the Harvard Law School Cyberlaw Clinic at the Berkman Center since its creation a decade ago. The Clinic provides innovative, hands-on training to Harvard Law students who, under careful supervision, offer legal and policy research, guidance and representation to a variety of real-world clients, including start-ups, institutional entities and research projects. Data and information privacy and security are foremost among the concerns, and the Clinic's attorneys and students frequently address novel questions of the practical application of privacy and data security laws, regulations and legal instruments to social science research initiatives.

- In October 2013, the Berkman Center announced participation in an innovative privacy program launched by Fordham Law School's Center for Law and Information Policy (CLIP). As part of the project, CLIP will release a curriculum for privacy education geared toward middle-school students. In coordination with Fordham, Berkman—particularly Youth and Media and the Cyberlaw Clinic—will adapt the curriculum and put the educational effort into practice.

Related Activities

In addition to the research and educational activities highlighted in the previous sections, the Berkman Center has engaged in various efforts aimed at shaping the state of privacy policy, technology, and organizational practice. Examples include:

- *Testimony and policy advice*: Berkman Center researchers have given testimony before policymaking and legislative bodies and international organizations such as the EU, OECD, and APEC (since 2007), particularly based on our Youth and Media work on youth, technology, and privacy as well as reputation issues as well our work on interoperability, which puts forth a nuanced theory of interop that considers the many benefits of increasing interconnectedness while also grappling with its potential negative effects, especially with respect to privacy.
- *Best practice models*: The Berkman Center was among the co-creators of the Global Network Initiative, a multi-stakeholder effort to protect and advance online privacy and freedom of expression, which draws on the international bill of rights to create overarching principles for ICT company decision-making. The GNI combines these principles with dy-

namic implementation guidelines and a supportive framework for learning and accountability to ensure that companies are behaving responsibly, and that their outcomes improve over time.

- *Prototyping new institutional models and research tools:* The Berkman Center's Law Lab (2008-2010) engaged in tool and institution building to deepen our understanding of trust, transparency and human co-operation.

Insights and findings from these and related efforts have been presented at many events in the US and abroad, including, for instance:

- *Hyper-Public: A Symposium on Designing Privacy and Public Space* brought together computer scientists, ethnographers, architects, historians, artists and legal scholars to discuss how design influences privacy and public space; how design shapes and is shaped by human behavior and experience; and how design can cultivate norms such as tolerance and diversity.
- Privacy-related events such as the *Future of Consumer Protection Workshop*, held in St. Gallen, Switzerland; a special speaker series on the Psychology and Economics of Trust and Honesty; and frequent presentations on privacy by guest scholars, including Berkman Fellows, as part of the Center's flagship event series.

Tax Status, Board Members, Key Staff

As a research center within Harvard University, the Berkman Center is recognized as a tax-exempt organization under Section 501(c)(3) of the Internal Revenue Code.

The Center is governed by its board of directors, which consists of faculty from across Harvard University. Chaired by Professor William Fisher of the Harvard Law School, the board includes Professor Yochai Benkler (Law School), Visiting Professor Susan Crawford (Law School, Kennedy School of Government), Professor John Deighton (Business School), Dr. Urs Gasser (Law School, Berkman Center Executive Director), Professor Charles Nesson (Law School), Professor Felix Oberholzer-Gee (Business School), Professor John Palfrey (Law School), Professor Jeffrey Schnapp (Faculty of Arts & Sciences, Graduate School of Design), Professor Stuart Shieber (School of Engineering & Applied Sciences), Professor Mark Wu (Law School), Professor Jonathan Zittrain (Law School, Kennedy School of Government, School of Engineering & Applied Sciences; elected Faculty Chair as of July 1, 2014).

The Center includes 30 full-time staff members as well as 61 Fellows and other Affiliates. We engage well over 100 students annually in our research and teaching programs directly, and classes taught by our faculty reach an additional 150 students each year. Key staff members include:

- Executive Director: Urs Gasser
- Research Director: Rob Faris
- Associate Director: Suzanne Kriegsman
- Director of Technology: Sebastian Diaz
- Clinical Program Managing Director: Christopher Bavitz
- Office Manager: Carey Andersen
- General Manager of Special Initiatives: Amar Ashar
- Project Coordinator: Geneve Bergeron

- Web Developer: Justin Clark
- Project Manager: Rebekah Heacock
- Project Manager: Jeff Hermes
- Project Coordinator: Adam Holland
- Digital Media Producer: Dan Jones
- Project Manager: Jennifer Jubinville
- Lead Engineer: David Larochelle
- Project Manager: Nathaniel Levy
- Systems Administrator and Platform Architect: Isaac Meister
- Financial Manager: Jon Murley
- Project Coordinator: David O'Brien
- Web Developer: Anita Patel
- Technical Support Specialist: Ed Popko
- Staff Assistant: Esther Simmons
- Project Manager: Alicia Solow-Niederman
- Financial Assistant: David Ssewankambo
- Manager of Community Programs: Rebecca Tabasky
- Research Associate: Shailin Thomas
- Clinical Instructor: Dalia Topelson
- Clinic Coordinator: Shannon Walker
- Project Coordinator: Dana Walters
- Web Developer: Ryan Westphal

Financial Disclosure

The Center is funded by numerous grants from private foundations and governmental agencies, with core support from the Berkman family, Harvard University, and contributions from individuals and corporations. All funds are managed by Harvard University and must

comply with the University's extensive financial guidelines, including segregation according to fund-based accounting principles, and are subject to annual external audit. As a matter of policy, the Berkman Center is committed to autonomy in our research and transparency in our relationships. These traits are essential to our continued credibility and success as an institution. Our funding model is possible due to the robust, strict, and clear policies that govern our association with donors and preserve the Berkman Center's intellectual independence.

Our research and outreach modes depend substantially on being able to convene and engage parties that span the spectrum of viewpoints, and for our research results to have impact, our work must not only be intellectually rigorous, but also fair and impartial. To that end, we do not accept grants that limit our ability to carry out research in the way we see fit—free of outside influence and consistent with our organizational mission and values. We do not undertake research or accept funds at the request of outside organizations unless it is consistent with our existing research agenda, mission, and overall philosophy. We are transparent about our funding sources, announcing the receipt of funds through our normal communication channels. For specific information, please see our website.

All corporate donors agree to give their funds as unrestricted gifts, for which there is no contractual agreement and no promised products, results, or deliverables. We have experimented with different arrangements at times in the past and have come to believe that this is the most productive approach for both the Center and our donors. These policies complement—and extend, in some respects—the relevant policies of Harvard Law School

and Harvard University. We will continue to review these policies to ensure that we are doing our utmost to maintain the integrity of the Berkman Center, our work, and our community.

Google, the defendant in this case, is among the nearly two dozen sources of current funding. In Fiscal Year 2013 (July 2012-June 2013), the Berkman Center received $307,500 from Google, which was approximately 3.9% of its total budget of $7.9 million for that year. In the current year, we have received $325,000 in contributions from Google as part of a $7.0 million budget, or 4.6% of the whole.

APPENDIX D

Efforts to promote online privacy via research and education at Carnegie Mellon

Lujo Bauer, Alessandro Acquisti, Nicolas Christin,
Lorrie Cranor, Anupam Datta

June 6, 2014

This document briefly describes the technical and societal impact of Carnegie Mellon research and educational efforts on online privacy, and proposes additional efforts in this space.

1. Carnegie Mellon University

Carnegie Mellon offers unique, world-class opportunities for security and privacy research. Carnegie Mellon hosts one of the largest academic security and privacy research centers in the world (CyLab), with over 50 faculty and 100 graduate students working on all facets of computer and information security and privacy, ranging from public policy to software design, to network measurements. To achieve high-impact research, inter-disciplinary collaborations between faculty and groups in drastically different fields (*e.g.*, psychology, economics and computer science) are not merely encouraged: they are the norm rather than the exception.

Ongoing privacy-related work in CyLab focuses on a number of different areas including understanding how Internet users make privacy-related decisions and providing tools to support them in making more informed decisions; using empirical data to evaluate the effectiveness and impact of privacy tools, privacy laws, and self-regulatory programs; and developing practical techniques to formalize and enforce privacy policies in various settings.

CyLab researchers have a strong track record in privacy research, outreach, and education. CyLab privacy research has appeared in top peer-reviewed conferences and journals and has been recognized with prestigious awards. Several privacy research papers by CyLab authors have been selected as "privacy papers for policy makers" by the Future of Privacy Forum. Recently, a paper describing empirical research on the effects of privacy information on online purchasing behavior coauthored by Acquisti, Cranor, and their students received the Information Systems Research award for Best Published Paper of 2012. In addition, privacy papers by CyLab faculty and their students are cited frequently in FTC privacy reports and at privacy-related hearings on Capitol Hill. Both Acquisti and Cranor have testified at privacy-related Congressional hearings, as well as at privacy workshops sponsored by the FTC and other Federal agencies. In addition, CyLab privacy researchers are frequently invited to present their research findings at companies—for example, faculty have recently given talks about their privacy research at Google, Facebook, PARC, and Microsoft. CyLab privacy research is mentioned frequently in the popular press, including theWall Street Journal, the Economist, The New York Times, Wired.com, and CNN; researchers have appeared recently on NPR and 60 Minutes, as well as on local television news programs.

CyLab researchers frequently teach privacy-related courses at the undergraduate and graduate level. Carnegie Mellon has recently launched the world's first masters degree program in privacy engineering. We expect that graduates of this is program will be well qualified to work for companies where they can help address privacy issues in products and services. As we developed the

curriculum for this new program, we talked to the privacy teams at a wide range of companies. They told us that it is difficult to hire employees with strong technical skills and a knowledge of privacy. Typically, they end up hiring software engineers or security engineers and providing some on-the-job privacy training. CMU privacy engineering graduates will be uniquely well qualified for privacy engineering jobs in industry. In order to attract top students to the privacy engineering program (rather than a more traditional software engineering or security engineering masters program), we have set up a scholarship fund so that we can provide some scholarship support to outstanding students.

2. Proposed efforts

Carnegie Mellon proposes a comprehensive effort to improve user privacy in an online setting. The research we propose to conduct can be divided into three categories: (1) furthering our understanding of users' privacy behaviors and online threats to users' privacy; (2) improving user-facing interfaces and technologies to increase users' understanding and control of their privacy; and (3) developing computational mechanisms to help ensure that systems and organizations adhere to privacy regulations or policies.

2.1 Understanding users' privacy behaviors and online threats to users' privacy

2.1.1 Evolutionary roots of privacy concerns and behaviors

We propose to explore, using a series of behavioral experiments, the influence that stimuli indicating the presence of other individuals in the physical world, often processed unconsciously, can have over security and privacy behavior in cyberspace. Our proposal is predicated around an evolutionary conjecture: human beings have

evolved to detect and react to threats in their physical environment, and have developed perceptual systems selected to assess these physical stimuli for current, material risks. In cyberspace, those stimuli often are absent, subdued, or deliberately manipulated by attackers. Hence, security and privacy concerns that would normally be activated in the offline world remain muted in cyberspace, and defense behaviors are thus hampered. Our proposal aims at investigating such conjecture and its potential implications, both in positive terms (what are the evolutionary roots of privacy and security behavior?) and in normative terms (how can we use that knowledge to improve privacy and information security in cyberspace?).

Our research question here is straightforward, while also ambitious: are there evolutionary roots for privacy and information security concerns, and can these roots be leveraged to improve privacy and security in cyberspace? While it is impossible to test such evolutionary conjecture directly, we can address the research questions by investigating the impact that external stimuli in the physical world have on security and privacy behavior in cyberspace. We plan to conduct a series of human subjects behavioral experiments aimed at investigating potential evolutionary roots of privacy concerns, and how the usage of physical and even visceral stimuli in the offline world can be used to assist privacy and security behavior in the online world.

Numerous factors determine our different reactions to real world and cyberspace threats. An act that appears inappropriate in one context (watching somebody undressing in their bedroom) is natural in another (on the beach); the physical threat of a stranger following us in the street is more ominous than the worst consequences

of an advertiser knowing what we do online; common sense and social conventions tell us that genuine Rolexes are not sold at street corners—but fake Bank of America websites are found at what seem like the right URLs. There is, however, one crucial parallel that connects the scenarios we just described: our responses to threats in the physical world are sensitive to stimuli which we have evolved to recognize as signals of danger. Those signals are absent, subdued, or deliberately manipulated in cyberspace. The evolutionary conjecture we therefore posit and experimentally investigate is that decision-making regarding privacy and security issues may be inherently more difficult in cyberspace than in the physical world, because (among other reasons) when we are online we lack, or are less exposed to, stimuli which we have evolved to employ in the real world as means of detection of potential threats.

We propose a series of lab experiments to investigate this conjecture indirectly—that is, by measuring the impact that the presence, absence, or changes, to an array of stimuli in the physical world have on security and privacy behavior in cyberspace. Specifically, human beings have evolved sensorial systems selected to detect and recognize threats in their environment via physical, "external" stimuli. These stimuli, or cues, often carry information about the presence of others in one's space or territory. The evolutionary advantages of being able to process and react to such stimuli are clear: by using these signals to assess threats in their physical proximity, humans reduce the chance of being preyed upon [9, 28]. Under this conjecture, the modern, pre-information age notion of privacy may be an evolutionary by-product of the search for physical security. Such evolutionary explanation for privacy concerns may help explain why—

despite the wide and diverse array of privacy and security attitudes and behaviors across time and geography—evidence of a desire for privacy and information security, broadly constructed, can be found across most cultures. Furthermore, since in cyberspace those signals are absent, subdued, or manipulated, generating an evolutionary "deficit," such an evolutionary story may explain why privacy and (information) security concerns that would normally be activated in the offline world are suppressed in cyberspace, and defense behaviors are hampered.

While we cannot directly test such an evolutionary conjecture (that the absence of stimuli that humans have evolved to detect for assessing threats, such as cues to the presence of other humans, contributes to our propensity to fall victim to cyberattacks or cyberspace privacy violations), we can test it indirectly. Namely, we can test—through a series of human subjects' experiments we have carefully designed—how the presence, absence, or modifications in an array of stimuli in the physical world affect security and privacy behavior in cyberspace. The term "stimuli," in the parlance of this proposal, is akin to the term "cues" as used in psychology and cognitive science.

Our experiments focus on three types of such stimuli: (1) sensorial stimuli: auditory, visual, olfactory cues of the physical proximity of other human beings; (2) environmental stimuli: cues that signal to an individual certain characteristics of the physical environment in which the individual is located, such as crowdedness or familiarity; and (3) observability stimuli: cues that signal whether the individual is possibly being surveilled.

The three categories are not meant as mutually exclusive (for instance, it is through our senses that we receive cues about the environment). Our experiments capture

how manipulations of the stimuli in the physical environment of the subject influence her privacy and security behavior in cyberspace. Privacy behavior is operationalized in terms of individuals' propensity to disclose personal or sensitive information, as in previous experiments by the authors. Security behavior is operationalized in a number of different manners, including susceptibility to cyber-attacks (for instance, phishing).

This significance of this research is two-fold. First, it attempts to advance the scientific understanding of what makes security and privacy decision making in cyberspace uniquely different from, and sometimes more difficult than security and privacy in the physical world, by introducing a novel approach to cybersecurity that takes into account the evolutionary roots of defender (and attacker) behavior in cyberspace. Second, by investigating a factor that may significantly disrupt user behavior in cyberspace, the research findings have applied relevance for developers, in that they can inspire how to construct systems that induce more secure behavior. Specifically, our aim is to provide design insights on the differences between perceived and actual security protection in cyberspace, and on how to make features of actual protection or invasion (which then affect choices and behavior in cyberspace) more salient.

Initial research in the above-described directions was funded by the National Science Foundation through a short (18 months) exploratory grant, which has been completed/expired. We ran some initial pilots, which produced promising results; we would use additional funds to design and run actual large-scale experiments based on the lessons learned from the pilots.

The findings of research could be used to examine whether physical stimuli can be used to ameliorate secu-

rity and privacy behavior in cyberspace. Security firms and any companies that develop software that allows its users to make privacy-related decisions could use visceral interventions informed by these results to improve users' ability to make secure and privacy-preserving decisions.

2.1.2 Impact of information leaks

We propose to investigate and quantify through measurement how private information leaks can impact online user experience.

For instance, we have observed through several measurement studies that an increasing number of websites were compromised by attackers who used them to redirect traffic based on the HTTP referrer field information [22, 23]. Somebody landing on one of these compromised websites from a Google search for a specific drug, would be sent to an online pharmacy; while on the other hand, different values in the referrer field would result in being shown the original, uncompromised, website. This mode of illicit advertising has considerably increased and become increasingly sophisticated over the past three years.

We are interested in systematically evaluating how adversaries can abuse information used a priori for user experience personalization (e.g., HTTP referrer), and what are possible countermeasures.

We have gathered evidence that "advertisers" as described above tend to be entities specializing in traffic brokerage. They are not, usually, the same entities as the ones which do sell products, but instead operate externally. For instance, somebody who operates an unlicensed online pharmacy would rely on an advertiser to bring traffic to their online store; that advertiser would

charge the pharmacist as a function of the traffic they manage to redirect to the pharmacy.

Uncovering the business of traffic hijacking In the context of our proposed research, advertisers are particularly interesting, in that they may be working for completely different types of businesses, seeking completely different types of customers. There is anecdotal evidence, for instance, that advertisers—also referred to as "traffic brokers"—charge differently based on the type of traffic desired. For instance, consider a traffic broker sending traffic to websites X and Y. If the operator of website X wants a mix of traffic from USA and Canada seeking pharmaceutical drugs, he probably does not pay the same price as the owner of website Y who is looking for Asian traffic reflecting an interest in adult movies.

We know very little about the specific types of information that is valuable to traffic brokers, and propose to conduct longitudinal, large-scale studies to try to determine how traffic is being monetized as a function of the perceived user interests. To that effect, we plan to build up on the measurement infrastructure we previously devised [22], to deploy it on machines all over the world, using the PlanetLab testbed [1], run queries for different types of traffic (adult, pharmaceutical, software, gambling, ...) and observe differences in a) the pages being fed to search engines as redirection points, and b) the pages on which we eventually land depending on the origin of the traffic.

Devising possible defenses We will then turn to evaluating possible countermeasures. Completely erasing the "HTTP referrer" field seems like a low-hanging fruit. We have, however, gathered anecdotal evidence that miscreants are able to exploit other types of infor-

mation (*e.g.*, cookies being set by landing pages in response to a given query [23]) to redirect traffic "intelligently" even in the absence of HTTP referrers. Informed by the measurements we will have gathered, we will attempt to reverse-engineer the various mechanisms being used, and, ultimately, design effective defenses against traffic hijacking.

The following outcomes of this research could be transitioned to practice:

- Thorough description of the traffic hijacking ecosystem; this could be useful to search engine operators such as Google, but also to law enforcement.
- Guidelines for traffic anonymization in order to avoid traffic hijacking. These could potentially be implemented as browser plugins or web proxies. Such an implementation would in turn be publicly available (open-source).

The research described in Section 2.1.2 would build on work partially funded by the National Science Foundation under award CNS-1223762 (2012-15). Specifically, that research has been to perform measurements evidencing the use of traffic brokers. We have also acquired anecdotal information these brokers perform traffic differentiation based on personal or private information surreptitiously obtained from their visitors; but we have not yet uncovered the types of private information that are valuable to brokers. This would require additional measurement studies as described in this section. These measurements are out of scope for the current NSF grant, and would only be possible with additional funding; similarly, the research on possible defenses and traffic anonymization at the end-host level would also be possible only with additional funding.

2.2 User-facing technologies to improve privacy

2.2.1 User authentication

A key aspect of the online experience is user authentication—in order to make online transactions (*e.g.*, online banking, email) users must first authenticate to a computer system, potentially giving up some privacy in the process.

One very simple solution to the problem of authentication is to use biometric authentication, in which an individual provides unique characteristics (*e.g.*, fingerprints, iris scan, . . .) to allow a different party to confirm their identity, and check that they are authorized to perform a given transaction.

The problem, however, is that this form of authentication binds identification with authorization: You must prove who *you are* to be able to conduct a transaction. While this binding may be desirable in certain contexts—for instance, access to critical physical infrastructure such as nuclear plants—it is actually a drawback for the vast majority of transactions conducted online, where users may desire privacy. For example, an individual purchasing condoms does not need, and probably does not want, their identity to be bound to that purchase for the purchase to be authorized. All that is needed is a proof that the payment instrument used for the purchase is valid and can provide sufficient funds.

Fortunately, ensuring that a certain individual is authorized to perform a transaction does not require to obtain details about the individual's identity; instead this authorization can be demonstrated by the knowledge or possession of an authentication token such as a password. In other words, authentication tokens allow to dissociate one's identity from the authentication mechanism, which

in turn allows for superior privacy guarantees. The challenge then becomes to design authentication mechanisms that are both usable and secure, while while simultaneously ensuring individual privacy is preserved.

Despite years of research trying to prove their obsolescence and replace them with more modern alternatives, authentication passwords remain a very strong candidate for meeting these security, usability, and privacy properties: Strong passwords are hard to break; everybody knows how to use a password; and passwords can be completely decoupled from one's identity. Unfortunately, very little is known about how to properly design guidelines for users to choose strong passwords that remain usable. While we have made advances in determining, for instance, how good a trade-off between usability and security long passwords (*i.e.*, passphrases) provide compared to complex password composition policies [20, 21], we still lack fundamental answers to important questions we propose to study.

Security of long passwords Longer passwords, which contain more characters are harder to crack by brute-force, *i.e.*, when the attacker tries to enumerate all possible passwords, which they can attempt to do in the context of offline attacks. They are also *a priori* more resilient than their shorter counterparts to more educated guessing [20], while being potentially easier to memorize. For instance, it is more straightforward to memorize "Mary had a little lamb," than "n!7#J*."

This comes from the property that the longer the password, the more structured it becomes: "Mary had a little lamb," for instance follows grammatical rules and can be modeled as "noun-verb-article-adjective-noun," which is a relatively common construction. Such constructions provide structure to long passwords, which in

turn makes them much easier to memorize; at the same time, an attacker could use such structures to considerably reduce the amount of guesswork they have to perform to discover a password. For instance, a structure such as "verb-verb-article-article" is probably exceedingly rare, and attackers would not need to try such combinations when attempting to guess a password.

We do not yet know the extent to which these higher-order structures (grammatical, or other mnemonic techniques users rely on) impact password security. For instance, is there a given password length that is short enough that users can shy away from relying on obvious structures, but long enough to provide strong guessing resilience? Are longer passwords always better? Can we gently nudge users into avoiding structural cues? Building up on our expertise in the area, we would rely on a combination of user studies and security analysis to find answer to all of these questions.

Impact of data entry interface Advocating longer passwords as more secure may be correct when data entry is simple; for instance, when a computer keyboard is used. However, the proliferation of mobile devices (cell phones, tablets) indicates that the assumption the data entry interface makes it easy to enter long passwords may be flawed. The increasing amount of private information those devices contain (pictures, contact information, and, increasingly, e-commerce transactions) makes it very pressing to device sound authentication technology for mobile devices.

Here again, we would need to conduct user studies to determine whether a) traditional passwords are a viable authentication mechanism on mobile devices, and if so, b) what are meaningful password composition policies for mobile devices. We would also need to pursue further re-

search in alternative authentication techniques; certain types of so-called "graphical passwords," for instance, could be a potential replacement worth considering [16].

Designing privacy-preserving fail-over mechanisms Another line of research well worth investigating is that of fail-over authentication mechanisms. Fail-over mechanisms take over when the principal means of authentication fails. For instance, a large number of email providers ask to provide answers to "security questions" (e.g., "what is your mother's maiden name?") so that users can bypass the password-based authentication mechanism and recover access to their accounts when they forget their passwords.

Fail-over mechanisms must thus be at least as secure as the authentication mechanism to which they serve as a back-up, lest an attacker would use them to gain unauthorized access. Security questions of the form described above have been shown to be an insecure mechanism, as most answers can be found with relative ease on social networks or other online resources. There has thus been a snift toward using "two-factor" authentication, where the back-up channel may for instance be a one-time password sent to a mobile device the user possesses. Unfortunately, because mobile devices are intrinsically personal, back-up authentication channels relying on them tie back a given user's identity to the authorization mechanism: differently stated, people may not be particularly inclined to divulge their personal cell phone number to an online service for fear of being tracked.

As part of this effort, we would try to design fail-over mechanisms that both provide privacy assurances, while simultaneously achieving a similar—if not higher—level of security as the primary means of authentication (*e.g.*, password-based authentication).

Online single sign-on The difficulty—for both users and service providers—of managing passwords has led to the increasing popularity of single sign-on mechanisms, which allow users to authenticate themselves to an *identity provider* (IdP); the IdP in turn vouches for the user to multiple *service providers* (SPs), absolving service providers of the need to authenticate users themselves. This frees users from remembering many sets of credentials, and frees service providers from the need to develop and maintain their own authentication mechanisms.

When a user logs into a service provider using an identity provider, the latter sends or authorizes the former to access a set of attributes about the user. Entities like Facebook and Google are starting to be widely used as identity providers by service providers such as Flickr and USA Today. Both Facebook and Google have social networking capabilities that make them uniquely qualified to provide rich information about users to service providers. Examples of attributes that may be conveyed from an identity provider to the service provider are age, gender, friend list, email address, current location, photos, and relationship status. The convenience to the user of using identity providers hence comes with a potential cost to privacy: the identity provider may send a service provider data that the service provider otherwise would not have known, and identity providers may learn yet more about users by keeping track of which service providers they access.

To address the former concern, identity providers like Google and Facebook explain to a user what types of information about the user will be sent to a service provider at (first) login. The types of information to be transmitted are typically displayed in a *consent dialog*, which gives the user a chance to abort the process of logging in

to a service provider if she does not want to share the described information with the service provider. A question that naturally arises in this context is to what extent identity providers in fact succeed at conveying to users what personal information they will share with service providers and give users the ability to make an informed choice. Early evidence suggests that users often do not realize how much privacy they are losing while using single sign-on mechanisms (*e.g.*, [3, 5]).

Through an iterative approach of designing new prototype interfaces and empirically evaluating them, we propose to develop interfaces that make the online single sign-on process significantly more transparent to users. Our goal will be to develop interfaces will allow users to make decisions about privacy that are well informed and consistent with their privacy concerns. We will explore the initial login or enrollment phase (*e.g.*, the first time a user clicks the "sign in with Google" button on USAToday.com), which most current interfaces focus on, but we will also develop interfaces to keep users more informed during follow up steps which are now often completely opaque to them (*e.g.*, subsequent logins to a service provider via an identity provider).

This research would potentially produce several artifacts that could be readily transitioned to practice:

- Practical guidelines for password composition policies that could be used by web services providers such as Google; beyond listing policies, we would also be interested in designing password meters that help users select better passwords, based on these guidelines. Such password meters could be open-sourced, and transitioned to anybody who is interested in using them.

- Improved, or novel authentication mechanisms for cellular phones and tablets. Prototypes would be designed to permit field evaluation, and could subsequently serve as a basis for implementation on production phones and tablets.
- New fail-over mechanisms that can be implemented by web service providers such as Google.
- A better understanding of how to communicate to users the privacy risks that accompany online single sign-on, as well as designs for improved and additional interfaces to communicate such privacy information to users.

The proposed research described in Section 2.2.1 on passwords builds on work supported in part by National Science Foundation award CNS-1116776 (2011-14), as part of which we have shown that long passwords can offer security without unduly compromising usability. That award is ending, and does not cover the specific research related to passwords described in this section. The proposed work on single sign-on builds on previous work funded by NIST, as part of which we demonstrated the inadequacy of current single-sign-on consent interfaces, including Google's [5] and developed a first prototype of a potentially more usable interface. Additional funds would allow us to run experiments to evaluate the initial interface, to iteratively refine it, and to explore ways to keep users informed after the first sign-in.

2.2.2 Smartphone privacy

An increasingly popular way for users to interact with the online environment is via smartphones and other mobile devices. We propose to conduct research to improve communication about privacy between smartphone app developers and their users, specifically with regards to

data collection, use, and sharing. Our research will build on our past research on privacy decision making and risk communication. Through a series of interviews with experts and lay users, surveys, and empirical user studies, we will inform the design of interface prototypes. We will iteratively design and evaluate interface prototypes and develop design recommendations for communicating privacy information to smartphone users. In addition, we will develop recommendations for tools for app developers that will improve their awareness of the privacy issues associated with their apps and facilitate better communication about privacy between app developers and their users.

We propose looking beyond users' preferences with location sharing [26, 29] or specific permissions [6, 13]. Furthermore, it is not our goal to identify or fix security holes in the Android system [2, 7, 8, 11, 12, 17, 33]. We will be examining the real harms that users are or should be concerned about with regards to smartphone data sharing. This research takes an approach that tries to determine the possible harms and privacy concerns that could occur to users through expert elicitations. With a holistic idea of the harms possible, we propose designing risk communications that allow users to understand the risks of harms compared to the benefits of data sharing.

As app developers are also important stakeholders, we will examine their choices about data collection when building apps. We will evaluate their resources and needs, and provide recommendations for tools that can assist app developers when making privacy and security decisions and communicating with users.

Consumer interfaces for understanding and control We will begin by interviewing experts on the causes and consequences of data sharing from smart-

phones. We apply methods of risk communication from the field of public policy to design notifications about data sharing on smartphones [25]. By interviewing experts in the field about actual harms and concerns to users, we will identify the most relevant decision points for consumers. The second step includes qualitative and quantitative work on users' understanding of data sharing. This will allow us to uncover the gaps between users' understanding and experts' judgment of risks and concerns.

We will implement and test several interfaces for providing notifications and configuration options related to data sharing from smartphones. This will include testing what information users understand, how to present it on a small screen, and the timing of notifications. Our evaluation methodology will be similar to approaches we have used in the past [18, 19], combining small-scale, qualitative laboratory studies and focus groups with large-scale, quantitative online studies.

Evaluating privacy notifications requires more than an evaluation of understandability. While understandability is a necessary criteria, it may not be sufficient for notifications to be successful. Furthermore, good notifications should assist users in making informed choices, but not necessarily lead them to being more or less permissive about what data is shared. We need to evaluate whether a person who uses the notice to make a decision, for example, about whether to install an app, is able to do so effectively. There are many factors that may determine whether a notice is useful, including whether people notice the notice, whether it is situated in a location such that users are still engaged in a decision process when they encounter it (as opposed to being already committed to installing the app), whether people understand what the notice means, whether the notice addresses the fac-

tors that people want to consider in their decision process, and more.

In one of our previous studies we told Mechanical Turk participants that their friend had recently purchased her first Android phone and wanted assistance in selecting some apps. She requested help selecting apps in six specific categories. We provided participants with a simulated Android store that offered a small selection of apps in each category with varying privacy levels. Participants in different experimental conditions saw different versions of a privacy notice. We were able to measure the extent to which each privacy notice caused participants to select apps with different privacy levels than they would select in the absence of privacy notices [19].

Building on the results of our studies, we will create design guidelines and best practices for smartphone risk communication.

As part of this work we will also identify any particularly vulnerable populations of smartphone users. For example, from preliminary work we have identified teenagers and the elderly as vulnerable populations. We will include investigations of their mental models about smartphone data sharing, and identify if and how risk communication should be designed to address their understanding and needs. As part of this project we expect to work with high school students at the Pittsburgh Science and Technology Academy, a public school focused on science and technology located near the Carnegie Mellon campus.

Tools for app developers While users may be concerned about data leakage, many app developers rely on collecting users' information in order to monetize their app. Currently, the ecosystem may create a conflict be-

tween monetization and privacy-sensitive apps. We will examine the data sharing decisions app developers make through a series of interviews and user studies with app developers. This will lead to a better understanding of the tools needed by app developers in order balance users' privacy concerns with the app developer' desire to innovate and monetize. We will propose tools and guidelines that will assist developers in creating apps that meet consumers' privacy needs.

Our research on communicating about smartphone security and privacy to consumers will result in a set of tested prototype notices and design guidelines. Software developers for mobile platform companies will be able to make use of these prototypes and guidelines to improve the way their platform communicates with users about privacy and security risk. In addition, we plan to develop privacy tools and guidelines for app developers and make them available for free. We will work with app developer forums and associations to make app developers aware of our tools. By increasing awareness about privacy issues among app developers and providing them tools that make it easier for them to build privacy into their apps, we expect to increase the number of apps that respect user privacy.

We have already reached out to representatives from the Application Developers Alliance[1] and Association for Competitive Technology[2], and hope to continue working with these app developer alliances as we propose new tools and interfaces.

We began our smartphone privacy research about a year-and-a-half ago with National Science Foundation

---

[1] http://appdevelopersalliance.org/

[2] http://actonline.org/

funds provided for PhD traineeships in Usable Privacy and Security. We are in our last year of funding for the traineeship program so the funding from this case will allow us to move beyond the preliminary phases of this project, complete our research studies, and develop useful design guidelines and tools.

2.3 Infrastructure for enforcing privacy policies

One approach to mitigating privacy concerns in the digital information age has been to enact laws (*e.g.*, HIPAA, GLBA). Another is for organizations to publish and adhere to self-declared privacy policies (*e.g.*, Google and Facebook in the Web services space).

One direction of our work at CMU has focused on investigating the possibility of formalizing and enforcing such practical privacy policies using computational techniques. We have formalized privacy policies that prescribe and proscribe flows (disclosures) of personal information [4, 10] as well as those that place restrictions on the purposes for which a governed entity may use personal information [30]. Recognizing that traditional preventive access control and information flow control mechanisms are inadequate for enforcing such privacy policies, we have developed principled audit and accountability mechanisms that seek to encourage policy-compliant behavior by detecting policy violations, assigning blame, and punishing violators. We have applied these techniques to several U.S. privacy laws and organizational privacy policies, including the first complete formalization of GLBA and the HIPAA Privacy Rule [10, 14]. In addition to developing algorithms and computer systems for privacy protection, we have initiated conversations with industry to transition these technologies. Specifically, we have presented our work to Google's Privacy Engineering team and generated significant inter-

est in joint work. Our methods for auditing disclosure clauses in privacy policies is of significant interest to Symantec; similarly, our work on enforcing purpose restrictions on information use is of significant interest to Microsoft.

We envision that we can conduct effective privacy research along these lines that will be directly relevant to improving compliance of Google's products (in particular, its search engine) with its privacy policies. Specifically, we will explore the possibility of checking that Google uses personal information for purposes that are compliant with their declared privacy policies. A central challenge that we plan to address is to enable this form of checking even when the checker does not have access to Google's software systems. This setting is particularly important because it will enable users, privacy advocacy groups, and government organizations to check that Google's practices respect users' privacy even though they will typically not have access to Google's internal systems. Such a tool will also help Google's internal privacy engineering team to detect potential compliance violations by studying the observed behavior of the system rather than its source code. This can be helpful in settings where third parties produce and maintain some of the software implementations that operate over personal information of Google's users. In taking on this challenge, we will build on our initial work on information flow investigations [31].

Concerns about privacy have led to much interest in determining how third-party associates of first-party websites use information they collect about the visitors to the first-party website. Mayer and Mitchell provides a recent presentation of research that tries to determine what information these third-parties collect [24]. Others

have attempted to determine what these third-parties do with the information they collect [15, 32].

The researchers involved in these works each propose and use various analyses to determine what information is tracked and how it is used. They primarily design their analyses by intuition and do not formally present or study their analyses. Thus, questions remain: Are the analyses used sound and/or complete? Are they related to more formal prior work?

To answer these questions, we must start with a formal framework that can express the problem and the analyses. In essence, each of these works is conducting an information flow analysis: the researchers want to know when information flows to a third-party and where it goes from there. Thus, the natural starting point for such a formalism is prior research on information flow analysis (IFA). However, despite the great deal of research on IFA (see [27] for a survey), we know of no attempt to relate or inform the research on tracking web trackers (TWT) with the models or techniques of IFA, even in an informal manner.

We believe this disconnect exists for an important reason: the traditional motivation for IFA, designing secure programs, pushes it away from analyzing third-party systems as done in TWT. Typically, the analyst is seen as verifying that a system under his control protects information sensitive to the system. Thus, the problems studied and analyses proposed tend to presume that the analyst has access to the program running the system in question. In TWT, the analyzed system is the adversary with the analyst aligned with a *data subject* whose information is collected by the system. In this setting, the analyst has no access to the program running the third-party service, little control over its inputs, and a limited

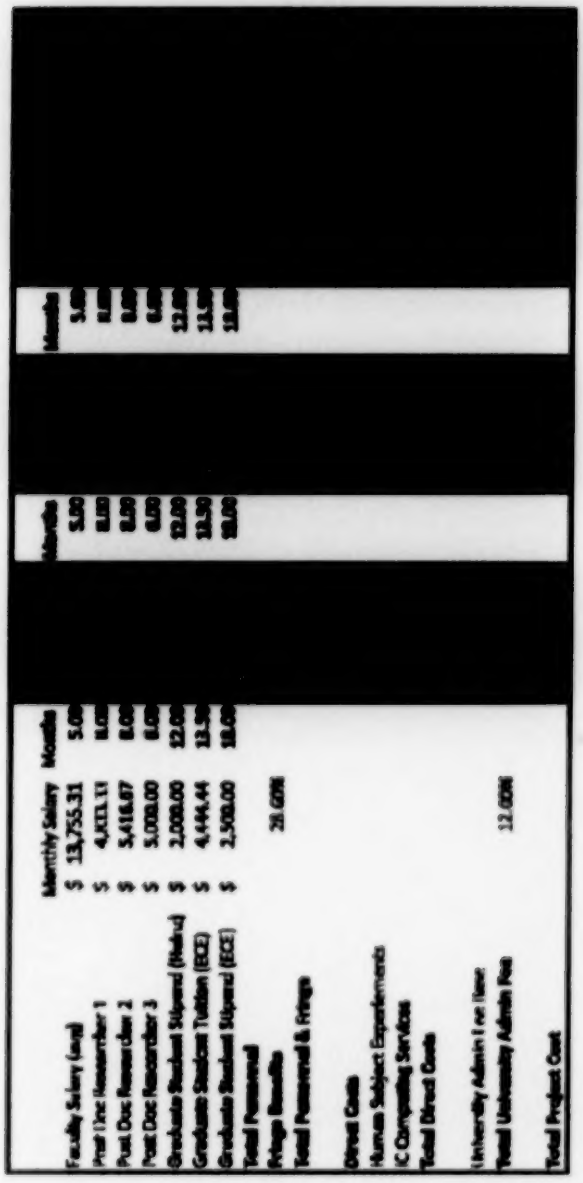
view of its behavior. Thus, the analyst does not have the information presupposed by traditional IFAs. To understand the TWT problem as an instance of IFA requires a fresh perspective on IFA. Our goal is to provide such a perspective by producing the following:

- A *theory of information flow investigations* that enables high confidence determination of whether a particular type of information (*e.g.*, a user's race or sensitive health information) influences the advertisements that he or she is shown by the advertising system. The theory will be statistical in nature and will enable this kind of determination based on evidence collected through experiments. This work will build on our prior work on this topic, which although a useful intermediate step in this direction is not statistical in nature [31]. A central idea is to construct a *differencing analysis* to enable discovery of information flows. This analysis in essence constructs two kinds of profiles that differ only in the type of personal information whose flow we are interested in (*e.g.*, race) and measures the difference in ads that are observed by the two profiles. The approach thus closely parallels how experiments are done in the natural sciences (*e.g.*, biology) to infer causality. There are numerous challenges involved in developing such a theory because of many confounding factors in the Web advertising ecosystem (*e.g.*, ad churn, geographic location) as well as the partial observability of the system (the analyst gets to only observe the behavior of the system on a small percentage of of the hundreds of millions of users who are served by the system).
- An *experimental methodology* and supporting *tools* that will enable analysts to conduct such studies. This contribution will enable others—internal auditors in

Web services companies, privacy advocacy groups, government regulators—to conduct such studies in the future to measure the privacy health of various Web-based systems that handle large volumes of personal information.

- A *validation* of the theory and experimental methodology by conducting a set of representative studies of an advertising system. The goal of these studies will be to discover the flows of personal information occurring in the advertising system, including those that are expected and those that are possibly not expected. These studies will help demonstrate the value of information flow investigations as well as to understand their limitations.

We plan to take active steps to transition the resulting technology to practice. As mentioned earlier, we believe that our experimental methodology and supporting tools will enable several different classes of stakeholders—internal auditors in Web services companies like Google, privacy advocacy groups, government regulators and even certain groups of Web users—to measure the privacy health of various Web-based systems that handle large volumes of personal information.



	Monthly Salary	Months		Months		Months
Faculty Salary (avg)	$ 13,755.31	5.00		5.00		5.00
Post Doc Researcher 1	$ 4,033.11	8.00		8.00		8.00
Post Doc Researcher 2	$ 5,418.87	8.00		8.00		8.00
Post Doc Researcher 3	$ 5,000.00	8.00		8.00		8.00
Graduate Student Stipend (Hybrid)	$ 2,000.00	22.00		22.00		22.00
Graduate Student Tuition (ECE)	$ 4,444.44	12.50		12.50		12.50
Graduate Student Stipend (ECE)	$ 2,909.00	18.00		18.00		18.00
Total Personnel						
Fringe Benefits	28.00%					
Total Personnel & Fringe						
Direct Costs						
Human Subject Experiements						
IC Computing Services						
Total Direct Costs						
University Admin Fee Here						
Total University Admin Fee	12.00%					
Total Project Cost						

Figure 1: Proposed allocations of funds.

Transition efforts will include actively interacting with relevant industry partners via visits and research collaboration (we have already initiated interactions with Google and have a record of successful transitions with other companies) and sending over students working on this project for industry internships; organizing workshops to disseminate project results to industry, government, and non-profit stakeholders (*e.g.*, we are organizing such a workshop in January 2014 jointly with MIT); and open-source release of resulting privacy-measurement tools.

The development of the methodology for information flow investigations has been supported in part by National Science Foundation grant CNS-1064688 (2011-15). The proposed project will expand the current effort by (a) producing a set of tools that automate the methodology enabling other researchers and practitioners to use these tools to conduct similar studies; and (b) conduct a set of comprehensive experiments to identify and measure flows of personal information in web advertising systems. We also plan to interact with Web services companies to explore avenues of use of these tools internally in these companies to proactively detect and correct unexpected flows.

3. Scope of effort and conflict of interest

Scope of effort We propose to carry out the described research over a period of three years. The scope of the proposed effort is approximately $1.25M divided evenly over the three years. This equates, per year, to 1 month of effort of each of the faculty, 50-67% of full-time effort of 3 post-doctoral researchers, 1.5 FTE (full-time-equivalent) PhD students. A detailed breakdown is shown in Figure 1.

The expected division of effort among the three thrusts is as follows: (1) furthering our understanding of users' privacy behaviors and online threats to users' privacy – 25%; (2) improving user-facing interfaces and technologies to increase users' understanding and control of their privacy – 55%; and (3) developing computational mechanisms to help ensure that systems and organizations adhere to privacy regulations or policies – 20%.

The precise allocation of effort and funds among researchers and thrusts may change depending on the needs of the research.

Conflict of interest As is common in academic research, several of the faculty involved in this proposal occasionally collaborate with and receive funding from various companies, including Google. Any particular collaboration does not affect the research directions we pursue outside of that collaboration, and no collaboration or relationship influences whether or which results of a scientific experiment or investigation we report. Hence, such relationships pose no conflict of interest with respect to the proposed research.

Specifically, of the faculty involved in the proposal, Alessandro Acquisti and Lorrie Cranor have both received funds from Google. In the past three years: in 2011, Cranor and Acquisti were among the CMU recipients of $178,920 as part of the Google Buzz privacy settlement, and, in 2013, a $15,000 gift to support a scholarship for the MSIT Privacy-Engineering masters program. We do not believe this causes a conflict of interest with respect to the proposed research. Any of the funding previously received from Google will not affect the scope, choice of research direction (in general or specifically), or outcome of the efforts described in this document.

4. Personnel

Alessandro Acquisti is an associate professor at the Heinz College, Carnegie Mellon University (CMU) and the codirector of CMU Center for Behavioral and Decision Research. He investigates the economics of privacy. His studies have spearheaded the application of behavioral economics to the analysis of privacy and information security decision making, and the analysis of privacy and disclosure behavior in online social networks. Acquisti has been the recipient of the PET Award for Outstanding Research in Privacy Enhancing Technologies, the IBM Best Academic Privacy Faculty Award, multiple Best Paper awards, and the Heinz College School of Information's Teaching Excellence Award. He has testified before the U.S. Senate and House committees on issues related to privacy policy and consumer behavior. Acquisti's findings have been featured in national and international media outlets, including the Economist, the New York Times, the Wall Street Journal, the Washington Post, the Financial Times, Wired.com, NPR, and CNN. His 2009 study on the predictability of Social Security numbers was featured in the "Year in Ideas" issue of the NYT Magazine (the SSNs assignment scheme was changed by the US Social Security Administration in 2011). Acquisti holds a Ph.D. from UC Berkeley, and Master degrees from UC Berkeley, the London School of Economics, and Trinity College Dublin. He has held visiting positions at the Universities of Rome, Paris, and Freiburg (visiting professor); Harvard University (visiting scholar); University of Chicago (visiting fellow); Microsoft Research (visiting researcher); and Google (visiting scientist). He has been a member of the National Academies' Committee on public response to alerts and warnings using social media.

Lujo Bauer is an Associate Research Professor in CyLab and the Electrical and Computer Engineering Department at Carnegie Mellon University. He received his B.S. in Computer Science from Yale University in 1997 and his M.A. and Ph.D., also in Computer Science, from Princeton University in 1999 and 2003. Bauer's research interests span many areas of computer security and privacy, and include building usable access-control systems with sound theoretical underpinnings, developing languages and systems for run-time enforcement of security policies on programs, and generally narrowing the gap between a formal, verifiable model and a practical, usable system. Much of his recent research has focused on understanding users' access-control and privacy needs as they interact with today's online services and on developing tools to help better meet those needs. Bauer recently served or is serving as program chair for the flagship computer security conferences of the IEEE (IEEE S&P 2015) and the Internet Society (NDSS 2014) and is an associate editor of ACM Transactions on Information and System Security.

Nicolas Christin is an Assistant Research Professor of Electrical and Computer Engineering at Carnegie Mellon University, and is affiliated with CyLab, Carnegie Mellon University's security lab. He also has courtesy faculty appointments in Engineering and Public Policy, and in the Information Networking Institute. He holds a Diplôme d'Ingénieur from École Centrale Lille, and M.S. and Ph.D. degrees in Computer Science from the University of Virginia, and did was a postdoctoral fellow at UC Berkeley. His research interests are in computer and information systems networks; most of his work is at the boundary of systems and policy research, with a slant toward security aspects. He has most recently focused on

online crime, security economics, and psychological aspects of computer security and privacy. He equally enjoys field measurements and mathematical modeling. His work on measurements of online criminal activity has garnered significant attention from the popular press (with NPR, Forbes, or the Economist among others citing various research efforts Christin led), but more importantly, helped the research community design much more accurate models of attacker behavior. Finally, his recent work on password authentication (jointly done with Lujo Bauer and Lorrie Cranor) is a successful example of integration of behavioral modeling with network measurements and mathematical analysis.

Lorrie Faith Cranor is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University where she is director of the CyLab Usable Privacy and Security Laboratory (CUPS). She co-directs the MSIT-Privacy Engineering masters program, the first graduate degree program in privacy engineering anywhere in the world. She has authored over 100 research papers on online privacy, usable security, and other topics. She has played a key role in building the usable privacy and security research community, having co-edited the seminal book Security and Usability (O'Reilly 2005) and founded the Symposium On Usable Privacy and Security (SOUPS). She also chaired the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C and authored the book Web Privacy with P3P (O'Reilly 2002). She has testified before Congressional committees and is regularly invited to brief federal agencies on privacy issues. Her privacy research is widely cited by both researchers and policy makers, and frequently mentioned in the popular press. She has served on a number of boards, including

the Electronic Frontier Foundation Board of Directors, and on the editorial boards of several journals. In 2003 she was named one of the top 100 innovators 35 or younger by Technology Review magazine. She was previously a researcher at AT&T-Labs Research and taught in the Stern School of Business at New York University.

Anupam Datta is an Associate Professor at Carnegie Mellon University where he holds a joint appointment in the Computer Science and Electrical and Computer Engineering Departments. His research focuses on the scientific foundations of security and privacy. Datta's work has led to formalizations of privacy as contextual integrity and purpose restrictions on information use; and accountability mechanisms for privacy protection. His research group produced the first complete logical specification and audit of all disclosure-related clauses of the HIPAA Privacy Rule for healthcare privacy. His group's work with Microsoft Research produced the first automated privacy compliance analysis of the production code of an Internet-scale system—the big data analytics pipeline for Bing, Microsoft's search engine. Datta's work has also led to new principles for securely composing cryptographic protocols and their application to several protocol standards, most notably to the IEEE 802.11i standard for wireless authentication and to attestation protocols for trusted computing. Datta has authored a book and over 50 other publications on these topics. He serves on the Steering Committee and as the 2013-14 Program Co-Chair of the IEEE Computer Security Foundations Symposium. Datta obtained Ph.D. (2005) and M.S. (2002) degrees from Stanford University and a B.Tech. (2000) from IIT Kharagpur, all in Computer Science.

References

[1] Planetlab. http://www.planet-lab.org.

[2] J. Andrus, C. Dall, A. Hof, O. Laadan, and J. Nieh. Cells: a virtual mobile smartphone architecture. In *Proc. of of SOSP 2011*, pages 173-187. ACM, 2011.

[3] M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila. Comparative eye tracking of experts and novices in web single sign-on. In *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 105-116, 2013.

[4] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum. Privacy and contextual integrity: Framework and applications. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 184-198, 2006.

[5] L. Bauer, C. Bravo-Lillo, E. Fragkaki, and W. Melicher. A comparison of users' perceptions and willingness to use Google, Facebook, and Google+ single-sign-on functionality. In *Proceedings of the ACM Digital Identity Management Workshop*, 2013.

[6] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pages 465-473, 2011.

[7] T. Blaandsing, L. Batyuk, A.-D. Schmidt, S. Camtepe, and S. Albayrak. An Android application sandbox system for suspicious software detection. In *5th International Conference on Malicious and Unwanted Software (MALWARE)*, pages 55-62, 2010.

[8] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani. Crowdroid: behavior-based malware detection sys-

tem for Android. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pages 15-26. ACM, 2011.

[9] C. Darwin. *On the Origin of Species*. John Murray, London, UK, 1859.

[10] H. DeYoung, D. Garg, L. Jia, D. K. Kaynar, and A. Datta. Experiences in the logical specification of the HIPAA and GLBA privacy laws. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society (WPES)*, pages 73-82, 2010.

[11] M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu, and D. Wallach. Quire: Lightweight provenance for smart phone operating systems. In *Proceedings of 20th USENIX Security Symposium*. USENIX Association, 2011.

[12] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of the USENIX Symposium on Operating Systems Design and Implementation*, October 2010.

[13] A. Felt, S. Egelman, and D.Wagner. I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns. Technical report, UCB/EECS-2012-70, EECS Department, University of California, Berkeley, 2012.

[14] D. Garg, L. Jia, and A. Datta. Policy auditing over incomplete logs: theory, implementation and applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 151-162, 2011.

[15] S. Guha, B. Cheng, and P. Francis. Challenges in measuring online advertising systems. In *10th ACM*

SIGCOMM Conf. on Internet Measurement, pages 81-87, 2010.

[16] E. Hayashi, N. Christin, R. Dhamija, and A. Perrig. Use your illusion: Secure authentication usable anywhere. In *Proceedings of the Fourth Symposium on Usable Privacy and Security (SOUPS'08)*, pages 35-43, July 2008.

[17] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In *Proc. CCS*, pages 639-652. ACM, 2011.

[18] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *CHI '10—Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Proc. of CHI 2010, pages 1573-1582. ACM, 2010.

[19] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. In *CHI'13—Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3393-3402, 2013.

[20] P. G. Kelley, S. Komanduri, R. Shay, M. L. Mazurek, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, pages 523-537, May 2012.

[21] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of

password-composition policies. In *CHI'11—Proceedings of 2011 ACM Symposium on Computer-Human Interaction*, pages 2595-2604, May 2011.

[22] N. Leontiadis, T. Moore, and N. Christin. Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. In *Proceedings of the 20th USENIX Security Symposium)*, pages 281-298, Aug. 2011.

[23] N. Leontiadis, T. Moore, and N. Christin. Pick your poison: Pricing and inventories at unlicensed online pharmacies. In *Proceedings of the 14th ACM Conference on Electronic Commerce (EC'13)*, pages 621-638, June 2013.

[24] J. R. Mayer and J. C. Mitchell. Third-party web tracking: Policy and technology. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 413-427, 2012.

[25] M. Morgan, B. Fischhoff, A. Bostrom, and C. Atman. *Risk communication: A mental models approach*. Cambridge University Press, 2001.

[26] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12*, pages 5:1-5:15, 2012.

[27] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5-19, 2003.

[28] M. Schaller, J. Faulkner, J. Park, S. Neuberg, and D. Kenrick. Impressions of danger influence impressions of people: An evolutionary perspective on individual and collective cognition. *Journal of Cultural and Evolutionary Psychology*, 2(3-4):231-247, 2005.

[29] E. Toch, J. Cranshaw, P. Hankes-Drielsma, J. Springfield, P. G. Kelley, L. F. Cranor, J. Hong, and N. Sadeh. Locaccino: a privacy-centric location sharing application. In *Proceedings of the 12th ACM international conference adjunct papers on Ubiquitous computing – Adjunct, Ubicomp '10 Adjunct*, pages 381-382, 2010.

[30] M. C. Tschantz, A. Datta, and J. M.Wing. Formalizing and enforcing purpose restrictions in privacy policies. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 176-190, 2012.

[31] M. C. Tschantz, A. Datta, and J. M. Wing. Information flow investigations. Technical Report CMU-CS-13-118, Carnegie Mellon University, 2013.

[32] C. E. Wills and C. Tatar. Understanding what they do with what they know. In *2012 ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 13-18, 2012.

[33] R. Xu, H. Saıdi, and R. Anderson. Aurasium: Practical policy enforcement for Android applications. In *Proceedings of the 21st USENIX Security Symposium*, 2012.

APPENDIX E

PRIVACY PREPAREDNESS PROJECT:

A proposal of the Center for Information, Society and Policy (CISP) at IIT Chicago-Kent College of Law

I. Introduction

The Center for Information, Society and Policy (CISP) at IIT Chicago-Kent College of Law is honored to be considered for funding from the cy pres award arising out of *Gaos and Italiano* v. *Google* (N.D. Cal.). The funds would enable us to undertake a project, PRIVACY PREPAREDNESS, which is a combination of academic research, public education, and outreach to safeguard individuals' online privacy and to help people, if they so choose, implement privacy protections when they interact with the web.

Americans care more about internet privacy than ever before[1] but may not realize when their online activities have implications for their privacy or how to choose among various technologies, apps, programs and settings to implement the level of privacy protection that they desire. This project will create interactive online materials and continuously update them for that task and roll them out across the country through videos, social media and in-person training sessions.

The project will alert people to the ways in which their privacy may be compromised on the web and offer them a range of choices about the level of privacy protection they can pursue. Through an interactive website and regular blog, it will offer advice about the privacy protections offered by various operating systems, browsers, add-ons, social networks, encryption tools, and risk assessment tools (to determine the safety of websites). For example, what are the relative merits of Twitter vs. Fa-

cebook in terms of the company's commitment to privacy? Android vs. Apple iOS in terms of allowing people to control what happens to their online data? What is NoScript, under what circumstances might I use it, and what are the steps to install it? How is all this going to change my experience with the web?

The project will also produce short videos and animations to inform people what is done with their information when they undertake web searches, play online games, and use social media.

II. Need for the Project

People post personal information about themselves on the web and reveal intimate information about themselves through their searches. Currently, many people do not understand that what they are posting on the web, searching for through search engines, or revealing unwittingly when using apps can often be accessed by others. People have a misplaced trust that what they post is private. A *Consumer Reports* poll found that "61% of Americans are confident that what they do online is private and not shared without their permission" and that "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations."[2]

Data aggregators collect identifiable information about people and market that information. Acxiom has data on half a billion people from around the world. The company has an average of 1,500 pieces of data on each person, "everything from their credit scores to whether they've bought medication for incontinence."[3] Google collects information from its 60 products and services.[4] Nielsen, a global marketing and information research company, boasts that its "Online Measurement" service

provides clients with "a 360 degree view of how consumers engage with online media." The company explains, "Our approach doesn't stop at the computer screen because we understand that online audiences don't just consume digital 'cookies'—they're a shopper, a carpooling power mom, a TV watcher, a tweeter and a texter."[5]

Individuals have difficulty keeping track of the uses that will be made of their online data. Commentators have estimated that reading the privacy policies of all the apps, social networks and search engines that people use would take a person 76 days per year.[6]

Increasingly, judgments are being made about people based on their digital doppelgängers. Seventy-five percent of employers assess people's internet presence before offering them a job. One-third of employers have rejected applicants based on their online profiles—and many have said that a photo of a person with an alcoholic drink in hand means a definite rejection.[7] A person can be categorized as more or less creditworthy depending on whether she has shopped at a bargain store online or at a higher end store.

III. Why CISP

At CISP, we undertake academic research, aid people in assessing their online privacy risks, and help policymakers develop appropriate policies. CISP faculty have advised a variety of institutions and groups on issues of internet privacy, including national legal groups, reporters, medical groups, forensic organizations, prosecutors and defense attorneys, the National Organization of Bar Counsel, computer scientists, universities, and government agencies in the United States and abroad. They have given keynote speeches on the topic in the United States, Asia, Central America, and Eastern Europe.

They are regularly quoted in the media on issues of internet privacy. Faculty members Lori Andrews, Doug Godfrey, Richard Warner, and Hank Perritt have all written books that touch on different aspects of internet privacy.

CISP currently analyzes the role that privacy plays in the law as well as in society more generally. The historical analysis undertaken by CISP shows that, with virtually every new technology in the past 125 years, including the portable camera, wiretapping, and genetic testing, privacy was initially declared dead. Yet, because of the important value of privacy to society, courts and legislatures ultimately protected privacy over technology. What are the contours of privacy in today's world? CISP explores the role of privacy and its legal underpinnings. The importance and relevance of internet policy research is highlighted by a prior cy pres award channeled to IIT Chicago-Kent for work in this field and by a Greenwall Foundation grant awarded to Professor Andrews to analyze how private medical information is collected from people's social network sites, web searches, and credit card purchases; how that information may be used against them; and what policies are needed to protect them. The activities of CISP include:

A. Social Networks, Data Aggregation, and Privacy

CISP analyzes how data aggregation may advantage and disadvantage individuals and canvasses applicable laws. It assesses the impact of information from social networks in criminal cases, divorce cases, school cases, employment cases, and other settings.

B. Social Networks and Health Information

Funded by the Greenwall Foundation, CISP analyzed the types of health information that are collected by so-

cial networks and related data aggregators and how that information is disseminated to third parties and social institutions. It pointed out the paucity of protections for health information on social networks and described how policies might be developed to protect health information on social networks in a manner that is more in line with the protections for health care information in other settings.

C. A Social Network Constitution

Professor Lori Andrews has proposed a Social Network Constitution to deal with the right to privacy, freedom of association, right to a fair trial, right to connect and other rights online.

D. Children and Internet Privacy

Even though Facebook is not open to children under age 13, 7.5 million children under age 13 use the service. FourSquare, Instagram, and other platforms are also used by children. CISP assesses the social, psychological, and legal implications of children's use of the social networks and the internet. It also analyzes proposed policies affecting children's use of the internet.

E. Law School Seminar on Social Networks

Law students interested in the implications of Facebook, Twitter, YouTube, Instagram, and other new means of communicating can take a course about the technologies, the impact, and the laws that govern them. They can also take a seminar on Network Security and Privacy or courses on the application of technology law or intellectual property law to this emerging field.

F. Liaison with Other Researchers

Within the university, more than 40 faculty members work on issues related to social networks. These faculty members, who are from a wide range of fields, including

engineering, psychology, computer science, biomedical engineering, and law, meet regularly. The faculty and research fellows at CISP also engage in research with researchers at other universities and in the private sector.

To aid in its analyses, CISP often draws on the technology expertise of faculty members and students at its parent university. For example, the Federal Trade Commission reported that, of the hundreds of apps for children, few disclosed to parents the type of information that they collected. CISP faculty instituted a project with IIT faculty and engineering students in which children's apps were downloaded and their code analyzed to see what type of information (including geolocation information) was being collected about the children when they used the apps. This allowed CISP researchers to provide data at the request of members of the U.S. Congress and help devise proposed policy to protect children's online privacy.

G. Conferences on Internet Privacy

In March 2012, CISP hosted a conference at IIT Chicago-Kent College of Law called "Internet Privacy, Social Networks and Data Aggregation." Leaders in the fields of computer science, engineering, law, and internet security discussed how social networks blur the lines between socializing and advertising, how data are collected and used, what legal remedies have been most effective and what the future holds for consumers, companies and the courts. Over 150 people attended the conference.

In October 2012, CISP hosted a conference at IIT Chicago-Kent College of Law called "Under Watchful Eyes: Privacy and the Technologies That Track." The conference analyzed the legal, privacy, and ethical issues

surrounding the collection and use of geolocation data. Over 150 people attended the conference.

In September 2013, CISP co-hosted an international conference on the use of surveillance technologies in the investigation and prosecution of financial crimes—and the privacy implications of gathering and storing that data.

In February 2014, Prof. Andrews and CISP Legal Fellow Michael Holloway partnered with The Media Consortium, a network of independent, progressive news organizations, including Democracy Now!, Mother Jones, and The Progressive, to provide trainings to journalists on technological tools for privacy protection. Over 100 journalists attended the trainings, which included workshops on email encryption, the Tor anonymity network, mobile privacy apps, the SecureDrop platform for secure, anonymous document submissions, and general online privacy principles and practices. CISP and The Media Consortium recruited trainers from organizations including the computer science department at University of Illinois at Chicago, the Guardian Project, and the Electronic Frontier Foundation. The Media Consortium has indicated an interest in collaborating in further privacy trainings for journalists.

In April 2014, CISP co-hosted a medical apps conference at IIT Chicago-Kent College of Law, "Health on the Go: Medical Apps, Privacy and Liability." There are at least 40,000 medical apps[8], and 52% of smartphone users look up medical information online from their phones.[9] Private and sensitive information about people is collected through these apps and searches, yet this information is not protected by HIPAA. The conference brought together medical app developers, policymakers and privacy experts to address how best to build privacy protections

in medical apps and to advise consumers about what is done with the information they enter into medical apps and medical searches. At the conference, Illinois Attorney General Lisa Madigan commented, "Privacy must be baked in."

IV. The Proposed Project

For the proposed PRIVACY PREPAREDNESS PROJECT, we would develop materials and tools to help people protect their privacy online, develop additional resource materials, and undertake public and professional education.

These materials and tools will be available to everyone, everywhere via the web. In addition, hands-on outreach about the legal underpinnings of internet privacy and the choices that are available through technologies, apps, and programs to protect privacy will be offered at national and local meetings of legal groups, reporters, consumer groups, the public, forensic organizations, prosecutors and defense attorneys, universities, and government agencies.

A. Public and professional education about online privacy

The information the proposed project will make available to the public and to professionals will 1) expose vulnerabilities in the technologies, devices and apps that people routinely use, 2) describe the circumstances in which legal protections exist and the circumstances in which they do not, and 3) teach people how to protect themselves online, should they so desire, including which browsers to use, how to search, how to best prevent tracking, and how to encrypt particularly sensitive information.

The class of people represented in the litigation that gave rise to this cy pres award will be benefitted by the following efforts:

- **Materials, videos, and resources** on the website that show the risks to privacy online and demonstrate the ways to deal with them and a dedicated **Blog** and dedicated **Twitter account** that contain updated information about online privacy.
- **In-person training** and **train the trainers** sessions. The project will have national outreach. CISP will train trusted intermediaries to get the word out to consumers about how to protect their privacy. In collaboration with the national group of investigative journalists (The Media Consortium), CISP will train reporters on how to cover internet privacy issues, how to explain to consumers about how to protect their privacy and how the reporters can protect whistleblowers and other sources. Project personnel will also work with high school teachers to teach them the fundamentals of online privacy so they can train their students. A related aspect of the Project will involve shorter trainings for groups of judges, lawyers, leaders of nonprofit organizations, community groups, and policymakers.
- **Technological scrutiny** of new and existing apps to assess privacy risks.

Some of the outreach will take place in Chicago. Chicago is a highly-populated area with many high schools and colleges. It is the home of various national medical and legal organizations, such as the American Medical Association and the American Bar Association, and multiple media outlets. But the trainings will not be limited to the Chicago area. Over the course of the three-year project, the project director and the legal fellow (and/or

the people they have trained) will be able to make presentations at national meetings of organizations around the country. (See Appendix A about the project director for an indication of the types of national organizations she presents to.)

In addition, IIT Chicago-Kent Student Bar Association's social media program has been recognized nationally as a "model for social media initiative."[10] It can engage students in privacy-protective activities and serve as a model for other institutions of higher learning to train students about privacy preparedness. In turn, we can leverage the power of law students to train others at limited cost.

The faculty members affiliated with CISP at Chicago-Kent are particularly well-positioned to aid consumers to protect themselves on the web. Chicago-Kent has a history of leadership in the field of computer law and the impact of digital developments on consumers. For over 30 years, the law school has had a Center on Law and Computers. Even before personal computers, the web, social networks, and data aggregation, Chicago-Kent focused on determining the appropriate use of computer technology from the vantage point of the consumer. In 1978, Chicago-Kent's "Law Office of the Future Project" changed the delivery of legal services to consumers by using computers to improve the delivery mechanisms of routine legal services to those who were unable to afford lawyers. We were known as the computer law school in the 1980s, pioneered use of e-notebooks in the 1990s, and more recently, drafted a software interface (A2J Author) that is used in more than 40 states and 4 countries to enable those not represented by counsel to navigate through the legal system. Our work garnered the Amer-

ican Bar Association's Louis M. Brown Award for Legal Access in 2008.

Our initial project in computer law undertaken 35 years ago has served as a model for the types of projects CISP does today: combining law and technology to benefit consumers. This consumer rights emphasis has also provided the foundation for numerous grant-funded projects undertaken by Chicago-Kent faculty. For example, the law school has been entrusted with previous cy pres awards, including a $5 million award to represent people who have been discriminated against because they have diabetes. The diabetes project has involved litigation and counseling on proposed legislation, working with IIT technologists to develop technologies that aid people with diabetes, and training high school teachers on the medical and legal basics for dealing with children with diabetes.

B. Academic Research

In order to enhance the benefits of the PRIVACY PREPAREDNESS PROJECT, we will also undertake two types of research projects. The first will be studies that analyze threats to privacy and the pros and cons of current technologies, apps, encryption methods, and behaviors to safeguard privacy. The second type of research will be an analysis of the special privacy concerns related to particular groups and particular types of information. These groups will include children, women, journalists, and professionals (such as lawyers and physicians). The types of sensitive information would include health care information, legal information, political beliefs and sexual preferences.

The analysis of apps and other technologies to determine the extent to which they present threats to privacy will be aided by a part-time Technology Fellow. In the

past year, we undertook a study of 275 medical apps with the assistance of a postdoctoral science fellow and found that the vast majority of the apps studied did not have privacy policies available prior to downloading the app. The apps that did have a privacy policy available often did not provide helpful or easily understandable tools to control privacy. Of the 275 apps, only eight had privacy policies stating that the app used electronic safeguards for data protection, and only five had privacy policies stating that no personally identifiable information would be sold.

People's online searches can reveal potentially stigmatizing information about them. A person may be searching for a divorce lawyer or an AIDS clinic. Such information, if disclosed, might lead to discrimination against the person or other harms. In fact, the use of online information about a person can be so harmful that Finland now has a law prohibiting employers from Googling potential employees.

Geolocation information, which people may be unwittingly disclosing (for example, when the smartphone photo a person has taken has a digital geotag), can also be problematic. The Supreme Court held in *U.S.* v. *Jones*[11] that the collection of location information implicates the Fourth Amendment. Justice Sotomayor stated that location information "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." If you know where a person has made her calls from, you would know whether she was meeting with a competitor to her current employer, attending an Occupy rally, going to an abortion clinic, or engaging in other sensitive activities.

Health information is considered so sensitive that it is protected by a federal law, the Health Insurance Portability and Accountability Act (HIPAA), when it is in the hands of medical professionals and medical institutions. However, health-related information does not have that same protection on the web. Private information is not adequately protected online. The lack of adequate privacy safeguards may mean that identifiable data about people's medical conditions are revealed to third parties who may use that information to stigmatize them or discriminate against them. Beyond inadvertent data-sharing, intentional data-sharing might take place. Just as hospitals sell people's genetic data to biotech companies by selling tissue samples without their knowledge, data aggregators sell people's online medical data.

People may be denied certain opportunities, benefits, or goods based on health information that was collected about them online. An employer might turn down an applicant based on information posted on that person's Facebook page about a doctor's appointment, about the person's desire to get pregnant or because of the person's "liking" a non-profit association related to a particular disease, such as the Cystic Fibrosis Foundation. A nursing home might deny admission to someone who had done an online search for a particular disorder that the nursing home managers do not want to deal with. By aggregating online data about an individual, marketing and research entities create more precise portraits of that individual, which then may be used for discriminatory purposes. For example, life insurance underwriting has traditionally been based on urine and blood samples that provide indications about a person's health. But now some consultants are suggesting that those tests (which are expensive and time-consuming for companies to ad-

minister) should be replaced by information from social networks and other online sources. Deloitte Consulting, LLP reports that this predictive modeling approach could save insurance companies an estimated $2 to $3 million a year and can "shorten and reduce the invasiveness of the underwriting" process.[12] Among the data collected online about a person that have been delineated as possibly making the person ineligible for life insurance is that the person has friends who are skydivers.[13]

Not only health information, but also confidential legal information, may be insufficiently protected on the web. The majority of U.S. lawyers have social network pages. Among responding ABA member-lawyers, 81% said they use social networks for professional purposes; 33% of the group used Facebook and 14% used Twitter.[14] But if a client posts information to a lawyer's Facebook page, that information loses the protection of attorney-client confidentiality.

C. Conferences and White Papers

The project will also sponsor annual conferences open to the public, lawyers, policymakers, computer scientists, and others. Policy papers will be developed each year related to the conference topic and posted on the website. At past CISP conferences, we have been able to educate at least 150 people per conference in person and have offered a streaming version of the panels over the web to other people without charge.

Year 1: In addition to its own research projects, the PRIVACY PREPAREDNESS PROJECT in Year 1 will commission six white papers—policy papers from industry representatives, government representatives, public interest representatives, consumer advocates and others about novel technological and policy means of protecting privacy.

Year 2: Privacy Preparedness Conference. This conference will build off of the research completed in Year 1 to provide a framework to evaluate privacy risks in the use of technologies in various everyday contexts—government, schools and children, workplace, and private use. The conference will consider the innovative proposals suggested in the white papers.

Year 3: Privacy Policy and New Technologies conference. Facebook is barely a decade old. Who knows what technologies will be developed to enhance or invade privacy in the next few years? This conference, held in the third year of the project, will assess the most recent technologies and will analyze existing privacy legislation at the time of the conference in order to make policy suggestions. Particular attention will be placed on showcasing and analyzing technologies that have been introduced to enhance privacy.

V. Methodology and Evaluation Component

The project will involve legal research, technological assessments, and outreach. As a part of the technological assessments, we will rely on colleagues at our parent university, the Illinois Institute of Technology, with whom we have worked on issues of internet privacy and social networks in the past.

Chicago-Kent is well-positioned to assure visibility for this project for a number of reasons. The school has international experts in the fields of social networking, privacy, and information security, and its partnership with a technology institute provides additional backing and attention to the project. Additionally, the frequency with which the project's faculty members appear on national television and in print, as well as Chicago-Kent's facility with social media and web communication, provides an advantage.

Most privacy materials posted by nonprofits, legal groups, or news organizations exist in relative stasis once developed, and only receive a small part of the organization's marketing and web communication goals. The online Privacy Preparedness Materials will be continually assessed and updated by lawyers and computer scientists and will have dedicated communications channels, including a dedicated Twitter account.

We will conduct evaluations as follows:

In-Person Trainings. CISP will keep track of the number of in-person training sessions and the number of program participants. The outcomes of the in-person trainings will be measured by before and after assessments of awareness among program participants of how participants can protect their privacy and the resources available to safeguard privacy. Project representatives will administer two surveys at the events. The first survey will assess the knowledge base of program participants before the trainings commence. The second survey will assess the program participants' knowledge at the completion of the trainings. The second survey will also ask questions regarding the effectiveness of the training format and whether the program participants found the information helpful and applicable. (We have used this method with respect to outreach trainings in the context of a cy pres award in a different field of law.)

Conferences. The effectiveness of the conferences at reaching people can be assessed based on the number of attendees and also based on the traditional surveys IIT Chicago-Kent distributes to attendees for evaluation after each of its conferences. These surveys were developed to comply with the requirements of state bars for the evaluation of continuing legal education.

Privacy Preparedness Materials. With the consent of participants, the project will keep track of the number of times the privacy materials and videos have been accessed online, downloaded or shared through social media, mentioned in the press or used by policymakers.

The project will similarly keep track of the number of visitors to the website, @ mentions, re-tweets (RTs) and favorites received. CISP will also look at citations of IIT Chicago-Kent College of Law work and mentions of the project in popular press. Finally, CISP will keep track of invitations from media organizations to discuss news events related to privacy and invitations to panels and symposia at academic and other relevant conferences.

VI. Risks and Opportunities

As with any project, there is a risk that we will not be able to reach our target audience. But CISP faculty and researchers have good relationships with reporters, the legal community, and others who will help us get the word out. There is a risk that the technology will evolve quickly, raising new privacy challenges. However, our strategy of having evolving materials on our website and of consulting technology experts at our parent university, the Illinois Institute of Technology and nationally, will help us keep in touch with the technology and tailor our advice and analyses accordingly. We have organized training sessions for educators at Chicago-area high schools, have organized large scale conferences, have spoken at a large number of academic and non-academic conferences, and have been interviewed by media reporters. There will be opportunities to expand the reach of the project, however, with our train the trainer model and our use of social media itself (Twitter, YouTube, and so forth) to increase the audience for the project's products.

VII. Personnel

The proposed project faculty are leaders in the field of internet and privacy law—Professors Hank Perritt, Harold J. Krent, Richard Warner and Lori Andrews. The director of the PRIVACY PREPAREDNESS PROJECT will be Professor Lori Andrews (who will devote half her time over a period of three years to the project). The project will also include the full-time services of a privacy legal fellow for three years. A staff of three part-time law student research assistants and a part-time Technology Fellow will also be paid from the project.

Project Director **Lori Andrews** is a Distinguished Professor of Law at IIT Chicago-Kent College of Law and the author of *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Internet Privacy*. She developed a Social Network Constitution, accessible at www.socialnetworkconstitution.com. She blogs regularly on the issues of internet privacy and has written articles on internet privacy for *The New York Times*, *Playboy*, *Cosmopolitan*, and other publications. She has spoken on the issues related to internet privacy to national organizations of lawyers, judges, law enforcement agents, prosecutors, defense attorneys, professors, scientists and doctors. She has appeared on panels with key people in the internet privacy community—on a four-person panel sponsored by *The New Yorker* with Pablo Chavez, the Director of Public Policy at Google; on a panel at the University of California, Los Angeles with Rob Sherman, Manager of Privacy and Public Policy at Facebook and FTC Chairman Jon Leibowitz; and in other settings with Marc Rotenberg of the Electronic Privacy Information Center (EPIC), FTC Commissioner Julie Brill and Julie Samuels of the Electronic Frontier Foundation (EFF). She has sponsored

conferences with speakers such as Christopher Soghoian, Harvard professor Harry Lewis and Lee Rainie of the Pew Research Center's Internet and American Life Project. (See Appendix A for Professor Lori Andrews' qualifications.)

Professor **Richard Warner** has written extensively on privacy issues, including a recent book on privacy and security with Robert Sloan, entitled Unauthorized Access: The Crisis in Online Privacy and Information Security, Chapman and Hall/CRC, July 2013. Professor Warner has assisted Professor Andrews with two privacy conferences: *Internet Privacy, Social Networks and Data Aggregation* on March 23, 2012, and *Under Watchful Eyes: Privacy and the Technologies That Track* on October 5, 2012. (See Appendix B for Professor Richard Warner's curriculum vitae)

Professor **Henry (Hank) Perritt** is the author of law review articles and books on technology and the law, including Law and the Information Superhighway (Aspen Publishers 2d. ed. 2001), and Digital Communications Law, one of the leading treatises on Internet law. (See Appendix C for Professor Henry H. Perritt's curriculum vitae)

Dean and Professor of Law **Harold J. Krent** focuses his scholarship on legal aspects of individuals' interaction with the government, and has written several articles and book chapters on privacy. In analyzing the question of the government's monitoring of e-mail and other online activities, Dean Krent and Professor Perritt were members of the 2000 IIT interprofessional team that examined the FBI's e-mail surveillance system (formerly known as "Carnivore") for privacy implications. (See Appendix D for Professor Harold J. Krent's curriculum vitae)

Legal Fellow **Michael Holloway** joined CISP in November 2013. Michael is involved in research projects on the uses and dangers of remote computer access tools and on the laws applicable to "revenge porn" and other extortion websites. In February 2014, Michael presented a workshop on the Tor anonymity network as part of a series of trainings for journalists on privacy protection tools. Michael prepared materials on FDA and FTC regulation of mobile medical apps for CISP's recent conference, *Health on the Go: Medical Apps, Privacy, and Liability*. Michael graduated in 2011 from Columbia Law School, where he worked on the *Columbia Science & Technology Law Review*.

Contact information for key personnel:

Lori B. Andrews
Distinguished Professor of Law
Illinois Institute of Technology Chicago-Kent College of Law
565 West Adams Street, Room 530A
Chicago, Illinois 60661
landrews@kentlaw.iit.edu
Telephone: (312) 906-5359

Harold J. Krent
Dean and Professor of Law
Illinois Institute of Technology Chicago-Kent College of Law
Office of the Dean
565 West Adams Street, Room 330
Chicago, Illinois 60661
hkrent@kentlaw.iit.edu
Telephone: (312) 906-5010

Richard Warner
Professor of Law
Illinois Institute of Technology Chicago-Kent College of Law
565 West Adams Street, Room 845
Chicago, Illinois 60661
rwarner@kentlaw.iit.edu
Telephone: (312) 906-5340

Henry H. Perritt Jr.
Professor of Law
Illinois Institute of Technology Chicago-Kent College of Law
565 West Adams Street, Room 713
Chicago, Illinois 60661
hperritt@kentlaw.iit.edu
Telephone: (312) 906-5098

VIII. Funding

We seek $949,875 over a period of three years to allow us to undertake a PRIVACY PREPAREDNESS project—a combination of academic research, public education, and outreach to professionals in order to safeguard consumers' online privacy.

We are requesting **$297,486** during **Year One**, which is broken down as follows:

- ***Salaries/Fringe.*** Funds will support time buyouts for one Director/professor of law (50% time), one professor of law (5% time), a second professor of law (5% time), one full-time legal fellow (100% time), three part-time research assistants, and one part-time technology fellow (at $25,000). We estimate salaries of personnel and fringe benefits will total $272,411.

- ***Activities***. Funds will support expenses for trainings of journalists and teachers for an estimated amount of **$8,000**. We will also commission six white papers at $2,000 each from distinguished policymakers and technologists for the second year conference (6 x 2,000 = **$12,000**).
- ***Supplies***. Funds will support supplies, including books, relevant publications, photocopy, postage, and food and refreshments at meetings. We estimate **$676**.
- ***Travel***. Funds will support travel for personnel—specifically airfare for attendance at trainings, meetings, or briefings. We estimate **$4,400**.

Note: In efforts to mitigate costs, we have not included all the staff and faculty time contemplated for this project. Our Director of Institutional Projects, and Assistant Dean of Administration and Finance will work on this project, and we will be drawing, without charge, on the expertise of Harold J. Krent, Dean and Professor of Law. In addition, we will not charge overhead costs.

We are requesting **$336,421** during **Year Two**, which is broken down as follows:

- ***Salaries/Fringe***. Funds will support time buyouts for one Director/professor of law (50% time), one professor of law (5% time), a second professor of law (5% time), one full-time legal fellow (100% time), three part-time research assistants, and one part-time technology fellow (at $25,000). Taking into consideration an approximate 2% salary and benefits increase, we estimate salaries of personnel and fringe benefits will total **$277,858**.
- ***Activities***. Funds will support expenses for the Privacy Preparedness Conference bringing together pol-

icymakers and technologists and focusing on the white papers commissioned the year before. We estimate conference expenses will total **$44,663** taking into consideration lodging, meals/incidentals, ground transportation and general meeting expenses. Funds will also support additional trainings of journalists and teachers. We estimate **$8,000**.

- ***Supplies***. Funds will support supplies, including books, relevant publications, photocopy, postage, and food and refreshments at meetings. We estimate **$1,500**.
- ***Travel***. Funds will support travel for personnel—specifically airfare for attendance at privacy conferences, trainings, or briefings. We estimate **$4,400**.

Note: In efforts to mitigate costs, we have not included some of the staff and faculty time to be spent on this project. Our Director of Institutional Projects, and Assistant Dean of Administration and Finance will work on this project, and we will be drawing, without charge, on the expertise of Harold J. Krent, Dean and Professor of Law. In addition, we will not charge overhead costs.

We are requesting **$315,968** during **Year Three**, which is broken down as follows:

- ***Salaries/Fringe***. Funds will support time buyouts for one Director/professor of law (50% time), one professor of law (5% time), a second professor of law (5% time), one full-time legal fellow (100% time), three part-time research assistants. Taking into consideration an approximate 2% raise, we estimate salaries of personnel and fringe benefits will total **$257,405**.
- ***Activities***. Funds will support expenses for the Privacy Policy and New Technologies Conference bringing together experts in cutting edge technologies and

privacy policy. We estimate conference expenses will total **$44,663** taking into consideration lodging, meals/incidentals, ground transportation and general meeting expenses. Funds will also support the last year of journalist and teacher trainings. We estimate **$8,000.**

- ***Travel.*** Funds will support travel for personnel—specifically airfare for attendance at privacy conferences, trainings, or briefings. We estimate **$4,400.**
- ***Supplies.*** Funds will support supplies, including books, relevant publications, photocopy, postage, and food and refreshments at meetings. We estimate **$1,500.**

Note: In efforts to mitigate costs, we have not included all our projected costs: Our Director of Institutional Projects, and Assistant Dean of Administration and Finance will work on this project, and we will be drawing, without charge, on the expertise of Harold J. Krent, Dean and Professor of Law. In addition, there will be no overhead charges.

REVISED Google Settlement – Preliminary Budget

Privacy Prepardness

IIT Chicago-Kent College of Law

Center for Information, Society and Policy (CISP)

Total Budget
Total 3 Year Period

	Award
Personnel	**673,978**
Fringe	**133,695**
Activities	**125,326**
Consultants	**0**
Supplies	**3,676**
Travel	**13,200**

IX. Conflicts of Interest

To our knowledge, no professor or staff member at IIT Chicago-Kent has a personal relationship with anyone at Google. Moreover, IIT Chicago-Kent to our knowledge never has received direct funding from Google. The law school benefited indirectly from a Google grant to then Northwestern University Professor Jerry Goldman's Oyez Project in that Professor Goldman subsequently joined our faculty.

Moreover, to our knowledge no professor or staff member at IIT has any personal connection with Google. Google has helped sponsor a number of modest technology projects over the years at IIT, including $40,000 in sponsored research toward a Pacific Island schools connectivity initiative in 2012, $1,500 to help defray the costs for a technology conference in 2011, a $10,000 gift to the Computer Science Department in 2010, and a $4,000 gift to the Computer Science Department in 2005.

---

[1] Rebecca J. Rosen, "Are the NSA Revelations Changing How We Use the Internet?" *The Atlantic*, August 19, 2013, http://www.theatlantic.com/technology/archive/2013/08/are-the-nsa-revelations-changing-how-we-use-the-internet/278830/.

[2] "Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy," Sep. 25, 2008, www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[3] Eli Pariser, "The Filter Bubble: What the Internet Is Hiding from You," 7 (New York: Penguin, 2011).

[4] Erik Sherman, "Google Will 'Scan' Your Email, Not 'Read' It. What Hypocrisy," *CBS News*, Oct. 27, 2010, www.cbsnews.com/8301505124_162-43446393/google-will-scan-your-email-not-read-it-what-hypocrisy/; "FAQ About Gmail, Security & Privacy," http://support.google.com/mail/bin/answer.py?hl=en&answer=1304609#data_retention; Abhineet Shukla, "Do You Know How Many Products & Services Does Google Have," Apr. 22, 2011, http://seo-trends-tricks.blogspot.com/2011/04/do-you-know-how-many-products-services.html; Jon Mitchell, "Google Puts +1 on Ads, Cre-

ates Google Plus Revenue Stream," ReadWriteWeb, Sep. 20, 2011, http://www.readwriteweb.com/archives/google_puts_1_on_ads_creates_google_plus_revenue_s.php; Sarah Kessler, "Google+ Enhanced Ads Are Up to 10% More Effective, Says Google," *Mashable*, Mar. 6, 2012, http://mashable.com/2012/03/06/google-plus-ads/; "Privacy Policy," http://www.google.com/policies/privacy/.

[5] "Online Measurement," http://nielsen.com/us/en/measurement/online-measurement.html.

[6] Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, March 01, 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[7] Cross-Tab, "Online Reputation in a Connected World." January 2010, http://download.microsoft.com/download/C/D/2/CD233E13-A600-482F-9C97545BB4AE93B1/DPD_Online%20Reputation%20Research_overview.doc.

[8] Jenny Gold, "FDA Regulators Face Daunting Task as Health Apps Multiply," *USA Today*, June 24, 2012, http://www.usatoday.com/news/health/story/2012-06-22/health-apps-regulation/55766260/1.

Susannah Fox and Maeve Duggan, "Tracking for Health," Pew Research Center-Pew Internet & American Life Project, at 2 (January 28, 2013), http://pewinternet.org/~/media//Files/Reports/2013/PIP_TrackingforHealth_PDF.pdf.

[10] Kevin O'Keefe, "IIT Chicago-Kent Student Bar Association: Model for social media initiative," *Lexblog: Real Lawyers Have Blogs*, February 18, 2013, http://kevin.lexblog.com/2013/02/18/iit-chicago-kent-college-of-law-student-bar-association-model-for-social-media-initiative/

[11] *U.S.* v. *Jones*, 565 U.S. ___ (2012).

[12] Mike Batty, Arun Tripathi, Alice Kroll, Cheng-sheng Peter Wu, David Moore, Chris Stehno, Lucas Lau, Jim Guszcza, and Mitch Katcher, "Predictive Modeling for Life Insurance: Ways Life Insurers Can Participate in the Business Analytics Revolution," Apr. 2010, www.soa.org/files/pdf/research-pred-mod-life-batty.pdf.

[13] Mike Fitzgerald, "Underwriting Using Social Networking Tools," Apr. 14, 2010, http://insuranceblog.celent.com/2010/04/underwriting-using-social-networking-tools/; Alice Kroll and Ernest Testa, "Predictive Modeling for Life Underwriting," May 19, 2010,

www.soa.org/files/pd/2010-tampa-pred-mod-4.pdf; Leslie Scism and Mark Maremont, "Insurers Test Data Profiles to Identify Risky Clients," *The Wall Street Journal*, Nov. 18, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

[14] Robert Ambrogi, "Lawyers' Social Media Use Grows Modestly, ABA Annual Tech Survey Shows," *LawSites*, August 5, 2013, http://www.lawsitesblog.com/2013/08/lawyers-social-media-use-continues-to-grow-aba-annual-tech-survey-shows.html.

APPENDIX F

Proposal For Distribution of *Cy Pres* Funds To Stanford Law School's Center for Internet and Society

Executive Summary

This proposal is an application for cy pres funds distributed in connection with litigation over Google's data sharing practices in the Google Referrer Header case. Particularly in the United States, Internet policy imagines end users have the knowledge, sophistication, and tools to protect themselves from unwanted information disclosure. This "notice and choice" approach has guided policy for two decades. Unfortunately, notice and choice has repeatedly failed users, leading to an erosion of trust online and a flood of privacy surprises. The Center for Internet and Society works in the public interest to empower and support user choice online.

We propose four projects designed to improve users' ability to make online privacy decisions for themselves. First, we focus on mobile privacy. Cell phones have become embedded in our daily lives, but the data flows they create are opaque and offer even fewer privacy controls than those of desktop computers. This leaves users all the more dependent on privacy policies. Yet small mobile device screens make it difficult for users to effectively read privacy policies. We propose original research to advance best practices for mobile privacy. Second, we focus on barriers to self-help approaches. Privacy Enhancing Technologies (PETs) enable users to enact their online privacy preferences. However, a range of well-known barriers reduce PETs use. Barriers range from tricky installation to lack of usability to simple lack of knowledge that PETs exist. We will run controlled trials

to see which barriers are the most significant, in order to improve existing and new PETs development.

Third, we will analyze proposed privacy legislation. Particularly in California, members of state legislatures are attempting to fix online privacy problems with legislation. We support the idea of limited legislation as a tool to create a minimum floor of accepted practices, but we notice several proposed bills are not technically feasible. We believe our mix of legal and technical expertise could be particularly valuable to lawmakers. Finally, we propose an educational speaker series. Users cannot make decisions for themselves when they do not know how their privacy is at risk. We propose public outreach to educate, inform, and train people about both online privacy risks and available tools to mitigate those risks.

In Part I: Introduction (page 2) we introduce ourselves. We describe the Center for the Internet and Society, our current and past work including projects related to online privacy, and our direct relevance to this litigation, the Google Referrer Header case. In Part II: CIS's Cy Pres Proposal Project Descriptions (page 8) we outline our funding request. We detail the three projects set forth above, as well as funding for the personnel required to conduct them, including Project One: Mobile Privacy Research (page 8,) Project Two: Barriers to Privacy Enhancing Technologies (page 9,) Project Three: Privacy Legislation Analysis (page 11,) and Project Four: Speaker series (page 13.) We conclude with Part III: Potential Conflicts (page 16.)

Part I: Introduction

By way of this proposal, the Stanford Law School Center for Internet and Society (CIS) is seeking distribution of *cy pres* funds to CIS in *In re: Google Referrer Header Privacy Litigation*, Case No. 10-cv-04809 EJD. CIS is a

public interest technology law and policy program and a part of the Law, Science and Technology Program at Stanford Law School. We currently have seven staff members, not including our faculty director, Professor Barbara van Schewick. They are Associate Director Elaine Adolfo, Director of Copyright and Fair Use Julie Ahrens, Director of Civil Liberties Jennifer Granick, Director of Privacy Dr. Aleecia M. McDonald, and Resident Fellows Giancarlo F. Frosio (intermediary liability,) Bryant Walker Smith (robotics,) and Legal Assistant Amanda Avila. In addition to our faculty director and staff members, CIS has affiliate scholars and non-residential fellows who study privacy and other civil liberties. They contribute to our blog, events, and publications. They are listed here:<http://cyberlaw.stanford.edu/about/people>.

History of the Center for Internet and Society

CIS has been in existence for 14 years. Founded in 2000, CIS is a non-profit organization that works to improve technology law and policy through ongoing interdisciplinary study, analysis, research and discussion. CIS brings together scholars, academics, legislators, students, programmers, security researchers and scientists to study the interaction of new technologies and the law. CIS strives to inform the design of both technology and law in furtherance of important public policy goals such as privacy, free speech, innovation and scientific inquiry.

CIS's Mission

CIS's goal is to improve technology law and policy through ongoing interdisciplinary study, analysis, research and discussion. We currently focus on copyright and fair use, network architecture and public policy, and privacy. In addition, we are building our competencies in government surveillance and intermediary liability policy. In order to engage in the current and future policy

questions that arise in these areas, CIS engages with the broader Stanford University and Silicon Valley communities, to produce high quality research, analysis, arguments and tools for stakeholders seeking to understand, promote and protect civil liberties and the public interest.

Relevance of Our Work to *In re: Google Referrer Header Privacy Litigation*

The United States' policies for online privacy focus on a few sectoral laws, plus a "notice and choice" approach. *Notice* requires companies state what data they collect and how they use it. Users may then make informed *choices* about data collection and use, often with technological *privacy tools* assisting them. The notice and choice approach is particularly challenged by *third party* data flows, that is, information that goes to a company that a user did not visit online, and may know nothing about.

In these class action cases, Plaintiffs allege that the notice and choice approach did not work. Google did not document the full details of their data practices. Plaintiffs were unaware that the information they searched for was passed from Google to third parties. Thus, Google disclosed the class' search terms to advertisers without their knowledge or authorization. This kind of information sharing between a first party (Google search) and multiple unknown third parties (advertising partners) in ways unknown and invisible to Internet users, is unfortunately common.

To address this problem, the class members, and all Internet users, need more effective means of receiving notice about the privacy practices of the services with which they interact. Class members, and all Internet users, also need more effective tools to control use and transfer of their information online. When users have

notice and tools, users can exercise greater control over their data and enforce their privacy preferences in their online interactions.

CIS's consumer privacy work strives to protect an individual's sensitive personal information from unwanted sharing or disclosure by improving both notice and tools. We study the strengths and weakness of a notice and consent regime for protecting online privacy, explore how to more effectively inform consumers about how a company uses and shares personal information with third parties, and create software tools to enhance user control over their personal data.

CIS's History of Success In Improving Consumer Privacy

CIS's research in consumer privacy has forged a direct path from scholarship to positive changes for Internet users.

Notice

There are many problems with privacy policies, including users' mistaken belief that a link to a privacy policy means they are protected by law,[1] difficulty reading and understanding privacy policies,[2] and the overwhelming amount of time it would take to read policies.[3] Despite

---

[1] Turow, J. Americans & Online Privacy: The System is Broken. Annenberg Public Policy Center Report, 2003 and reproduced in Hoofnagle, C.J. and King, J. What Californians understand about privacy online, 2008.

[2] Jensen, C. and Potts, C. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *CHI '04, Proceedings of the SIGCHI conference on Human factors in computer systems* (New York, NY, USE, 2004,) ACM, pp. 471-478.

[3] McDonald, A. M., and Cranor, L. F. The cost of reading privacy policies. *I/S – A Journal of Law and Policy for the Information Society 4*, 3 (2008.)

these obstacles, privacy policies are the most prevalent way for Internet companies to communicate their online practices, and users' best sources of information. The challenge, then, is how to go from information buried in a privacy policy to information that users can notice, process, and use to make decisions. As in *Google Referrer*, the Class must know about data practices in order to decide to allow them or limit them.

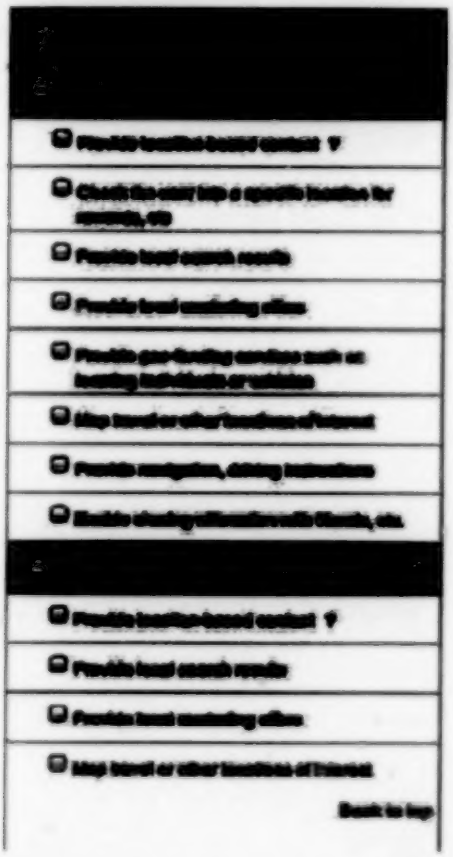


Figure 1: TRUSTe's mobile notice questions for authors

Effective privacy notice is even more challenging on small cell phone screens, and this is an increasingly important problem to solve. Mobile Internet access on smart phones and similar devices has expanded greatly. There are three times as many mobile broadband subscriptions as fixed broadband in the United States,[4] with nearly two thirds of US citizens using smartphones.[5] As with desktop search, Google dominates mobile search and is estimated to capture 70% of the funds spent on mobile search ads.[6] Mobile web browsing presents all of the same privacy challenges as desktop web browsing, plus includes new sources of information including geo-location, ambient sound, and motion sensing. Privacy controls on mobile devices have lagged. Users have experienced limited ability to ability to manage cookies, years with no ability to control data flows from apps, and a persistent lack of privacy policies.

The opportunity for mobile privacy work is to respond while the mobile ecosystem is still evolving in order to help developers create tools and notices that are practical and useful. At present, there is limited work on how to convey actionable privacy information to users on a small screen. As more users access online services over their

---

[4] International Telecommunication Union's *ITU's Global ICT Developments*, 2001-2013 (2012.)

[5] Lacoma, Tyler, Mobile Design, "Smartphone Penetration on the Rise Yet Again," (July 18, 2013.)

[6] mobiThinking, "Global mobile statistics 2012," referencing the International Data Corporation's study *IDC Predictions 2011: Welcome to the New Mainstream* (December, 2010.) Similarly, Gartner estimated Google's mobile advertising revenue represents 70% of the market in *Forecast: Mobile Advertising, Worldwide, 2008-2015* (March, 2011.)

mobile devices, making app and other mobile notices effective is a high priority. With the advent of novel devices like Google Glass and increased use of sensors in devices like personal fitness trackers, cell phone screens will seem large by comparison. In the future, cell phones are expected to become the "hub" to control many new devices with sensors, sometimes described as the Internet of Things (IoT). There is a pressing need to work on meaningful privacy communication for new situations. Members of the Class will use mobile devices to search and browse online, control their cars remotely, check on home security while traveling, and other applications not yet invented.

- Our Notice by Design work applies human-computer interaction research and experimentation to the problem of giving consumers effective notice of online privacy practices. This widely discussed research leverages legal expertise in privacy with post-graduate research in user interface design. The New York Times and New York Times Magazine have referenced our work. Some of its central insights, for example the idea of "visceral notice", have been implemented by household name Internet companies, positively effecting user privacy in relation to products we use every day. Former CIS Director of Privacy Ryan Calo's Notre Dame Law Review article on this topic, *Against Notice Skepticism (In Privacy And Elsewhere,)* was selected by the Future of Privacy Forum as one of six "Privacy Papers for Policy Makers" in 2011.

- Ryan Calo joined the faculty of the University of Washington law school in 2012 and Aleecia McDonald transitioned from Resident Fellow to Director of Privacy. Ryan remains a CIS affiliate and was recently awarded Best Paper at the 2013 Privacy Law Scholars Conference for his piece, "Digital Market Manipulation."

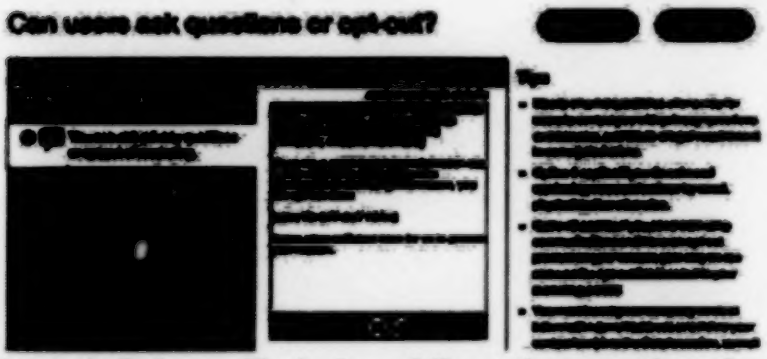


Figure 2: Privacy Choice's mobile notice questions for authors

- Aleecia and Ryan began research together on how best to present privacy notices on mobile phones and other devices, including testing existing tools from TRUSTe and Privacy Choice (see Figures 1 and 2). This resulted in a conference paper presented at the 40th Annual Telecommunications Policy Research Conference (TPRC 2012,) and a subsequent journal publication, McDonald, A. M., and Lowenthal, T. Nano-Notice: Privacy Disclosure at a Mobile Scale. *Journal of Information Policy*, Vol. 3 (2013), pg. 331-354.
- Aleecia served as a member of the State of California's Mobile Privacy Advisory Group in 2012-13. This group worked with the California Department of Justice (CalDoJ.) As a member of the Mobile Privacy

Advisory Group, Aleecia advised California officials on best practices and usability issues for mobile privacy notices. The state published guidelines including the Group's advice subsequent to CalDoJ negotiations with Apple, Google, HP, Amazon, Microsoft and RIM to ensure users of app stores could view privacy policies before installing mobile applications. Aleecia also testified about online privacy before the California State Assembly Select Committee on Privacy on March 19, 2013.

- Aleecia's research on the time it would take to read privacy policies, and the economic value of that time, established that privacy policies currently cannot adequately educate users and protect their data in practice. This work has been widely cited in the Washington Post, NBC News, The Atlantic, Slashdot, on NPR, in international press, in Federal Trade Commission (FTC) staff reports, and in a 2014 White House publication about Big Data.
- The National Science Foundation selected a joint project with Carnegie Mellon, Fordham Law, and CIS for one of two Frontier awards this year. The project includes interdisciplinary work to investigate how to take the information that currently exists in privacy policies and present it to users in ways that enable users to make better online privacy decisions.

Our research improves privacy notice practices, enabling Internet users, including the Class, to make educated choices about the privacy impact of their online activities.

Third Party Tracking and Data Flows

When users visit a website, like http://www.google.com to search online, that website is often formed from a mix of

content from multiple parties. For example, searching for "online privacy" brings results from many companies, including advertising that comes from companies other than Google. As most browsers are configured today, ads are able to set cookies on a user's computer. Cookies are small text files that often contain a unique identifier for the user, like a social security number. This lets the advertiser recognize the same user later on a different website, a practice known as *third party tracking*. Advertisers collect information about where they see users and what users are reading to build profiles of users' interests in order to show targeted advertisements. Some users find great benefit in ads that match their interests, but studies show the majority of users do not understand how data is collected or that it is shared with other parties, and do not wish to share their data.[7] This mirrors the experience of the Class members, whose search terms were disclosed to third parties without their knowledge, understanding, permission or control. CIS works on methods that put users in control of third party data collection.

- In 2010, the FTC called for a voluntary Do Not Track (DNT) system, which would give users means to express their preference to opt out of third party tracking online. In response to criticism that DNT was not technically viable, Jonathan Mayer (a junior affiliate scholar at CIS) and Arvind Narayanan (a non-

---

[7] McDonald, A. M., and Cranor, L. F. Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES)* (October 4 2010) and Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy and Hennessy, Michael, Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009.)

resident affiliate scholar at CIS, now on the Princeton faculty) created a prototype to demonstrate DNT. This prototype paved the way for all major browsers to add the ability for its users to send a DNT signal. The question then became what a website must do to honor an incoming DNT signal set by Internet users.

Aleecia co-chaired the WC3's Tracking Protection Working Group, an ongoing effort to establish international standards for a Do Not Track mechanism that users can enable to request enhanced privacy. This effort brings together over 100 international stakeholders including industry, academia, civil society, privacy advocates and regulators. The group is chartered to reach an open, consensus-based multiparty agreement that will establish a baseline for what sites must do when they comply with an incoming request for user privacy. However, despite three years of efforts, the stakeholders in the WC3 Working Group have not reached a consensus view of what DNT must do.

The fundamental impasse is that businesses no longer believe they can afford to limit data collection when DNT adoption rates approach 20%, and privacy advocates want DNT to strongly limit data collection and use. While CIS remains engaged in DNT work, it also seems time to try a new approach that does not require consensus agreements.

There is strong legislative interest in DNT. California AB 370 would require websites to declare how, if at all, they respond to a California user's Do Not Track request. On August 22, 2013, the California Senate voted 37-0 to approve AB 370. It came into force on January 1, 2014. Aleecia contributed to the California Attorney General's guidance on best prac-

tices for privacy notices, published in May, 2014, *Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy.* Aleecia is also leading research to study how companies respond to the legal requirements for DNT disclosure, and estimate how many times companies disregard users' requests not to be tracked.

Part II: CIS's Cy Pres Proposal Project Descriptions

To continue and expand our work on consumer privacy, CIS requests up to $971,400 in *cy pres* funds to conduct four projects over the next three years. The four projects are independent of one another allowing funding to scale up or down. However, all four projects are contingent on funding for personnel as described in the section below on Necessary Personnel.

Project One: Mobile Privacy Research

Our prior work investigated how two popular privacy policy systems that rely on icons to convey information compare to each other, as well as to text-only presentations. We find that icons coupled with text can be effective, but small screen size makes it vital to show the information that is of top priority to a user at the time she is making privacy decisions. Understanding what, when, and how to display information effectively remains a research area with great promise.

In February, 2012, the California Attorney General's office reached an agreement with six major mobile vendors to disclose privacy policies for mobile applications prior to download. The California Department of Justice and the Federal Trade Commission are both actively seeking solutions to the problem of how to provide working privacy notice on small cell phone screens.

CIS proposes to expand our research on best practices for user privacy notice to the context of mobile devices.

- Within two years we would complete human subjects research on how to prioritize and present privacy information and create one or more papers of publishable quality along the lines of Calo's highly successful paper *Against Notice Skepticism*.
- We will also investigate the potential efficacy of privacy enhancing technologies, technical standards, and possible legal requirements to limit data flows, in order to learn if there are methods other than notice that users might prefer.
- We would then promote adoption of the lessons of this research regarding effective mobile notice with app developers, as we did with "visceral notice" and websites.
- We would also work with lawmakers, for example at the CalDoJ and Federal Trade Commission to help them understand our research and use it in their regulatory work.
- We would host a training event for up to 100 app developers. By training 100 app developers, we can expect to see those app developers create offerings with improved privacy policies. We will measure success of this training through (1) the number of app developers offering privacy policies for the first time within a month of attending the Stanford workshop, (2) the number of apps with privacy policies that adopt our suggestions for usability within three months of the Stanford workshop, (3) the number of downloads of those apps, and therefore the number of individuals with greater transparency and understanding of data practices.

($98,000, includes cost to research technology and payments to research participants in a nationally representative study: $60,000 and one event to train app developers how to instantiate mobile privacy policy notice and choice for at least 100 people to be held at Stanford: $38,000.)

Relevance and Benefit to the Class

Effective notice is a precursor to effective choice. The Class members alleged that they were given neither notice nor choice about how Google would relay their search queries to third parties. As Internet users, including Class members, migrate to mobile devices, providing effective notice will directly improve their ability to control the flow of information about them. Currently mobile users do not understand how companies use, collect, or share information. Most mobile developers do not understand they are compelled by California law to document their data policies, and do not know how to go about doing so. It is not enough to tell mobile developers they must write privacy policies, we must also determine and demonstrate how to make privacy information useable. Rather than burying practices in an unread privacy policy, salient details must be presented to users in new ways, before they make privacy decisions.

Success metrics: We anticipate that our work will improve mobile privacy notice. Our metrics will be (1) whether the central insights of this research are implemented by household name Internet companies, as happened with "visceral notice" on desktop devices; (2) whether policy makers at the FTC or CalDOJ adopt and encourage companies to implement our research insights.

Project Two: Barriers to Privacy Enhancing Technologies

In what researchers have termed the "privacy paradox," users say they care very much about privacy, but do not avail themselves of existing self-help measures to ensure privacy. This phenomenon is less surprising in light of research that users mistakenly believe they are protected by privacy laws that do not exist, and users mistakenly believe companies would never risk reputational harm by engaging in common business practices to collect, store, share, and sell user data.

With the press coverage of Snowden's documents, Internet users are becoming more aware that their information online is not as private as they once imagined. As a result, users increasingly are turning to software tools to control information about them, including the terms they search for online, the websites they visit, and their reading habits (see Figure 3). These kinds of software are known as Privacy Enhancing Technologies (PETs) and are designed to put users in control of their information. The ultimate goal is not to protect privacy as much as possible, but rather to have users' online experiences match their privacy preferences.

However, there are many well-known barriers to PETs use. First, users need to know they have privacy risks. Second, they need to know there are ways to mitigate those risks. Third, they need to be able to install PETs, which is sometimes quite difficult. Finally, many PETs are cumbersome, slow, or difficult to use. PETs developers are often small groups of volunteers rather than professional software development teams. While PETs developers would like to make their products appeal to more than a small group of enthusiasts, PETs developers often lack the resources to address significant barriers.

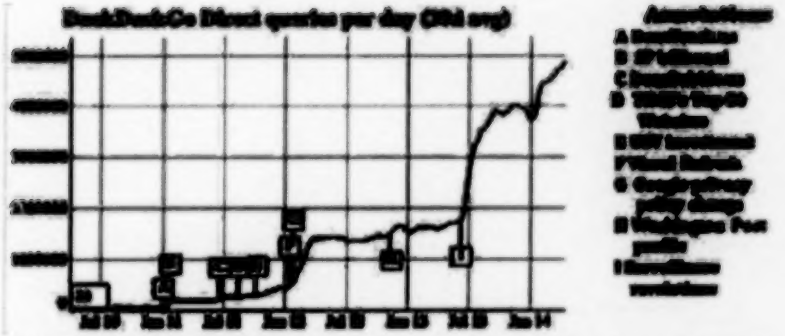


Figure 3: Duck Duck Go use jumped when Google changed their privacy policy and after press coverage of Snowden's documents.

We propose the first detailed research into the ways these barriers interfere with user adoption and use of PETs. Through a series of human subject experiments we will test pairs of configurations for PETs. For example, do research participants use PETs significantly more when installation is easier, or faster? Do research participants use PETs in ways that better match their privacy preferences when they understand how the software protects them, and how it might interfere with other features they like? To perform this analysis we will hire a part-time computer science student to create different versions of installation software for existing PETs, such as:

- Tor Browser, which limits information sharing on the web including masking IP addresses and not sending referrer headers
- DuckDuckGo, a search engine that does not track users
- Privacy Badger, a web browser plugin that blocks some forms of online tracking

- PGP, a difficult-to-use approach to encrypting email

Our research goal is to learn where PETs fail users, and which barriers to PETs use are most significant. Our results will help PETs engineers as they allocate their development resources. As a beneficial side effect, we may develop improved installation procedures or user interfaces in order to test them. We will contribute our improvements back to the development teams for each project whenever possible.

($64,400, includes cost to develop multiple variants of existing PETs ($30,000 for part-time students in computer science,) summer interns to perform research and analyze results ($14,400) and direct costs of $20,000 to perform research and pay participants.)

Relevance and Benefit to the Class

Effective privacy notices are necessary but not sufficient for users to enact their privacy preferences online. If the members of the Class had been aware their referrer header information was shared with advertisers, they could have taken steps to limit that sharing if they wished. PETs provide those steps to limit sharing. However, the members of the Class would still have experienced barriers to their efforts to use PETs to limit referrer header data collection. By researching which barriers to PETs use are more significant, we can improve PETs more rapidly, and create tools that are better able to meet the Class' privacy interests. This project is responsive to privacy choices generally, and also specifically to the referrer header issue.

Success metrics: We anticipate that our work will improve the PETs we study, and PETs overall. Our metrics will be (1) whether the central insights of this research are implemented by PETs development teams, as

happened with "visceral notice" on desktop devices; (2) publication of at least one high-quality research paper in a technical journal detailing the most significant barriers to PETs adoption and how to overcome them; (3) ongoing citations to research work, indicating diffusion of knowledge within the research community; (4) increased adoption of PETs when they meet users' privacy preferences, indicating success in lowering barriers to PETs adoption.

Project Three: Privacy Legislation Analysis

Privacy is a topic of increasing legislative interest. In 2012, the California legislature introduced nearly two dozen privacy bills. Many of these are well-intentioned bills that nevertheless would benefit from better understanding of underlying technical realities. Our interdisciplinary approach puts us in a unique position to inform the legislature on law, policy, *and* technology.

For example, the California Assembly is considering updates to the Shine the Light law, California Civil Code 1798.83. The goal is to increase transparency and understanding of data collection, including data transfers between first and third parties, which would help address issues of the Class. Unfortunately, the bill was drafted in a way that is technically infeasible for many companies, as it asks first parties to disclose information they typically will not have. With some work to redraft the approach, the bill it could be effective.

As another example, AB 242 is an act to amend Section 22575 of the Business and Professions Code to require privacy policies not exceed 100 words. The idea is that since privacy policies take too long to read, it would be better to force them to be short so users are more likely to read them. Unfortunately research shows short form privacy policies are less effective, since users assume anything not mentioned is not collected or used—

and companies cannot fit all of their data practices into 100 words. Part of the remedy for the Class is to give effective notice of privacy practices, yet this law would make it unlikely there would be enough room for that notice. Our work on effective mobile notice could help the legislature tailor this law to achieve its worthy goals.

[Figure omitted: "Making Your Privacy Practices Public" logo with seal of Kamala D. Harris, Attorney General, California Department of Justice]

Figure 4: We contributed to the AG's recommendations on Do Not Track, but lack resources for full policy engagement

Beyond California, the idea of a "right to be forgotten" online is a topic of great interest in Europe and in the U.S. (See, *e.g.* Representatives Markey and Barton's proposed "eraser button" in the Do Not Track Kids Act of 2011, H.R. 1895 (112th).) While many measures are targeted at preventing data collection, erasure proposals focus on deleting data after it has been collected, allowing a new set of remedies for unwanted data collection and distribution. In May, 2014 The European Court of Justice ruled that Google must provide access for users to delink information about themselves, which brings discussions away from mere theory. However, there are many challenges to implementing a "right to be forgotten," both technical and legal, including conflicts with freedom of expression.

While we have provided informal advice on some of the California bills, we have not had the resources to become more engaged, even as bill authors are open to input. Members of the Center for Internet and Society have strong relationships with state and federal policy makers. These relationships give CIS a path to be effective and influential in California privacy law.

With *cy pres* funding, we would publish at least three white papers responsive to privacy bills and proposed legislation under active consideration by state lawmakers. In addition to informal meetings with policy makers and briefings, we would also conduct at least one event that introduces academics and policy makers with knowledge transfer in both directions.

For this project, CIS would hire a full time legal fellow to help the Director of Privacy study pending bills and respond with published analysis in the form of white papers or publications. We would also hold a major event in cooperation with the California Assembly Select Committee on Privacy (or other appropriate partner) to bring together experts in privacy scholarship and legislative staff. (Human and technical resources for this project: $295,000—includes a full-time legal fellow for three years: $240,000, and events for $38,000.)

Relevance and Benefit to the Class: As awareness grows that online data collection is more pervasive than it appears, and as companies are vocal that they are unwilling to voluntarily limit online data collection and use, there is greater talk of legislation being the only recourse available to protect privacy interests. Without a sound technical and legal basis, privacy legislation may unnecessarily fail. The legislature risks passing laws that are impossible to implement or inadvertently harm the people they purport to protect. Because California claims jurisdiction over California citizens, any company that has a user located in California must follow California privacy laws for that user. In practice, it is too difficult to distinguish California citizens from all others, and too costly to create multiple systems. As a result, California privacy laws become de facto national laws. If the Shine the Light amendments and AB 242 were improved, these

laws could enhance transparency so members of the Class will know who collects their data and where that data goes.

Success metrics: Our goal would be to help policy makers author practical and implementable legislation, and to encourage academic researchers to contribute their thinking to relevant policy issues. Successfully passing legislation is outside of our control. However, we note that bills are routinely defeated because they are slightly incorrect at the technical layer. We see three types of success. (1) Legislative directors and policy makers attending the Stanford event would leave with greater technical understanding of how the web works. Much as users do not understand invisible data flows, legislators do not either. We will collect feedback forms at the end of the event to confirm participants have an enhanced understanding. (2) Introducing researchers and policy makers must be the start of a longer conversation, not the end. We will create a briefing book containing the biographies of participants, allowing ongoing contact over time. (3) Successfully working with legislators to amend or introduce privacy protecting bills that are technologically astute.

Project Four: Speaker series

[Figure omitted: CIS Tech Workshop 2014 logo with photographs of Monica Chen and Garrett Robinson]

Figure 5: Our first workshop of 2014 addressed invisible information flows

CIS has a popular lunchtime and evening Speaker Series. In 2011 we held four lunch talks and five evening talks. In 2012 we held four lunch talks and two evening talks. In 2014 we create a new series of hands-on workshops to teach attendees how to install and use privacy enhancing software tools. In addition, we invited promi-

nent speakers including renowned security expert Bruce Schneier and journalist Julia Angwin. We held a total of six evening events. See Figure 5 for one example. Our evening speakers have been much better attended by members of the public than our workshops or lunch events, but evening events are much more expensive to host, averaging $7000 each. Our events are professionally video-recorded and made available through our YouTube channel so that members of the public who cannot attend may still benefit from the events.

One aim of the Speaker Series is to foster public understanding of important privacy issues. If we are awarded this funding, CIS would host three additional evening events open to the public, specifically about consumer privacy online. Via these events, we both educate the public and introduce prominent privacy researchers to the general public, which is contact they may normally not have. In this way the speakers reacquaint themselves with the knowledge level and interests of people outside the privacy expert sphere. Consumer privacy topics relevant to the Class that we would host potentially include: (1) how the public can make effective online choices for privacy (2) how third party web tracking and behavioral advertising practices work and/or (3) how seemingly anonymous data can be used to re-identify people. ($21,000 for costs of three events.)

Relevance and Benefit to the Class: Education is a key aspect in putting users in control of the data they transmit. For example, Internet users who understand what referer (sic) headers are can opt to use technical means to suppress sending that information from some web browsers. These are advanced measures that require understanding how data flows work to even understand there might be an issue to address, let alone what

tradeoffs are involved. Our Speaker Series events can address these needs by educating users who are able to attend the speaker series in person, and also reaching a geographically remote audience as well.

Success metrics: (1) At least 300 people in attendance across all evening events, (2) at least three different top-notch speakers, (3) at least 100 remote attendees and downloads within a year of the event.

Necessary Personnel

With this *cy pres* award, CIS would make the position of Director of Privacy permanent. From June 2010 to July 2012, CIS had a full-time Director of Privacy who focused on consumer privacy. That former Director, Ryan Calo, left to join the faculty of University of Washington Law School. CIS funded our current Director of Privacy, Aleecia M. McDonald, for a two-year term ending 2014. While we have accomplished a great deal and brought about real changes in consumer privacy, funding remains limited. CIS anticipates that adding a permanent Director level position specifically for consumer privacy will enable CIS to accomplish the projects listed below, as well as other relevant research that would directly benefit the privacy interest of Class members in controlling the use and dissemination of their personal information. We also request a portion of the salaries of two staff members, Associate Director Elaine Adolfo and Legal Assistant Amanda Avila, to perform administrative tasks directly relevant to this *cy pres* request, including financial accounting for all research projects, managing travel and expenses for workshops and training sessions, running events and speaker series, and providing web design and maintenance. We do not seek general funding and do not request overhead. All expenses are directly tied to the privacy projects outlined above (Three year's

salary and benefits for a Director level position: $450,000. Portion of additional staff salary and benefits for three years: $60,000.)

Thus, the total CIS seeks in *cy pres* distribution from this litigation is $971,400, as detailed in Appendix A: Proposed Budget on page 18.

Part III: Potential Conflicts

Stanford Law School's development department researched any connections CIS, its umbrella organization the Law Science and Technology Program LST), or Stanford Law School might have with the parties or their attorneys. Stanford Law School has no financial or other connections with Paloma Gaos, Anthony Italiano, Gabriel Priyev, or Eric Schmidt (Plaintiffs) nor with Kassra P. Nassiri, Michael J. Aschenbrener, or Ilan Chorowsky (Attorneys.) Mr. Nassiri is a graduate of Stanford with a Master of Arts in Economics in 2000. Neither LST nor CIS have any financial connections with Judge Davila. The only Law School connection found is that, according to a White House press release dated May 20, 2010, Judge Davila taught trial advocacy at Stanford Law School before being appointed to the bench.

Contributions from the Parties.

CIS is part of the Law, Science, and Technology program, which has received funds from Google for work on patent law in 2013. Additionally, Google has donated funds to the Center for Internet and Society from 2006 to 2013. We do not believe these funds establish a conflict of interest.

All funding CIS receives is deposited into accounts controlled by Stanford Law School. Stanford Law School is fiscally responsible for and monitors the accounts. CIS

follows all law school and University policies and procedures for expending funds from our accounts.

Per Stanford University policy, all donors to the Center agree to give their funds as unrestricted gifts, for which there is no contractual agreement and no promised products, results, or deliverables. Stanford has strict guidelines for maintaining its academic autonomy and research integrity. CIS complies with all these guidelines, including the Conflicts of Commitment and Interest section of the Stanford Research Policy Handbook <http://doresearch.stanford.edu/policies/research-policy-handbook/conflicts-commitment-and-interest>. Stanford policies provide explicit protection against sponsors who might seek to direct research outcomes or limit the publication of research.

Since 2013, Google funding is specifically designated not be used for CIS's privacy work. CIS's academic independence is illustrated by the following work by Privacy Director Aleecia M. McDonald and CIS Junior Affiliate Scholar Jonathan Mayer, which may not accord with Google's corporate interests:

- Aleecia and Jonathan each contributed greatly to Do Not Track efforts, including demonstrating the technical feasibility of Do Not Track; leadership in the W3C standards process; and work with the California Attorney General's office on the language and enforcement of AB 370, California's law requiring corporate transparency regarding how they respond to Do Not Track signals. Do Not Track was an alternative to Google's preferred approach to make opt-out cookies persistent.
- Based on Jonathan's research, Google paid a record $22.5 million dollar FTC fine for circumventing users' privacy choices in Apple's Safari web browser.

- Jonathan wrote code to a change to the Mozilla Firefox browser to make it as privacy-protective as Safari. Jonathan's code is now part of the Firefox product. Aleecia created the Cookie Clearinghouse to expand upon Jonathan's improvements to Firefox. These changes could affect Google and other companies' revenues from targeted advertising.

For these reasons, we do not believe we have a conflict of interest with either Google or with the Plaintiff class.

CIS thanks the Court for the opportunity to submit this Proposal for consideration in the proposed settlement of this litigation.

I, Aleecia M. McDonald, am authorized by CIS Faculty Director Professor Barbara van Schewick to sign this proposal on behalf of CIS.

Dated: May 19, 2014 By: _____

Aleecia M. McDonald, PhD
Director of Privacy
Center for Internet & Society
Stanford Law School

Appendix A: Proposed Budget

Proposed Budget

Center for Internet & Society
Stanford Law School

	Year 1	Year 2	Year 3
Project One: Mobile Privacy Research			
Research technology, conduct nationally representative study	60,000		
Train app developers		30,000	
Project Two: Privacy Tools Research			
Half-time computer science student		15,000	15,000
Summer research intern		7,200	7,200
Conduct research, payments to participants		10,000	10,000
Project Three: Privacy Legislation			
Full-time legal fellow (salary plus benefits)	80,000	80,000	80,000
Events for policy makers and academics		30,000	
Project Four: Speaker Series			
Effective online choices	7,000		
How web tracking & advertising work		7,000	
Re-identification of anonymous data			7,000
Necessary Personnel			
Director of Privacy (salary, benefits)	145,000	150,000	155,000
Portion of Associate Director and Legal Assistant (salary, benefits) to run events, etc	20,000	20,000	20,000
Annual Total	$ 312,000	$ 365,200	$ 294,200
Total Request		$	971,400

Appendix B: CVs for Necessary Personnel

Aleecia M. McDonald
Director of Privacy
Center for Internet & Society
Stanford Law School

I research topics in Internet privacy and security. I work to contribute to a more coherent picture of how, why, and when people make choices about protecting themselves online, and what that means to them. My interests span users' mental models of online interaction, study of and creation of usable tools to support online decision making, and how people learn about and reason about online trust issues. In addition to technical tools, I focus on technically informed policy approaches in standards bodies, regulatory agencies, and legislation in the United States and European Union nations.

Education

Carnegie Mellon University Engineering & Public Policy Ph.D., September, 2010. Thesis: *Footprints Near the Surf: Individual Privacy Decisions in Online Contexts.* Committee members: Lorrie Faith Cranor (chair), Alessandro Acquisti, Deirdre K. Mulligan, Jon M. Peha.

Carnegie Mellon University H. John Heinz School of Public Policy and Management. M.S. in Public Policy and Management with a concentration in Internet Policy, May, 2006.

Carnegie Mellon University B.A., Professional Writing, 1993.

Employment

Stanford University Center for Internet & Society, Director of Privacy, staff position, 12/12 – present

Conduct privacy research. Directed three summer students (2013) in research regarding privacy access and correction rights, the "right to be forgotten" in the US and EU, and a quantitative analysis of the Chilling Effects database regarding the de-linking of copyrighted information. Created a hands-on privacy workshop speaker series covering Mozilla's Lightbeam, Tor, GPG, HTTPSEverywhere, and speakers on corporate and government surveillance. Created the Cookie Clearinghouse.

Successfully applied for the first-ever NSF funding for CIS, as part of a multi-university Frontier award.

Stanford University Center for Internet & Society, Resident Fellow, half-time staff position, 11/11 – 11/12

Under the direction of M. Ryan Calo, performed research regarding mobile privacy policies. Led efforts to standardize what it would take to comply with an Internet user's request not to be tracked online.

Mozilla Corporation, Senior Privacy Researcher, contract and part-time employment, 3/11 – 11/12

First hire into Mozilla's privacy team in the legal department. Worked with engineering to publish internal and external documents regarding Do Not Track implementations. Conducted research on privacy preferences for Mozilla Test Pilot users.

Carnegie Mellon University, Research Assistant, staff position, 5/06 – 8/06

Under the direction of Professor Jon M. Peha, managed a group of three students to investigate spyware traffic on the Carnegie Mellon network. Determined schedule and priorities for students. Used Snort on Red Hat with custom anonymization tools to ensure privacy. Responsible for IRB (Institutional Review Board) interactions.

Performed data analysis in mySQL, SAS, and R.

Center for Democracy & Technology, Summer Intern, 5/05 – 7/05

Authored two internal papers on RFID (Radio Frequency Identification) including research on security issues and privacy. Participated in events on layered privacy notices, Real ID, and the PATRIOT Act. Edited written comments to the Federal Election Committee. Attended FEC and Senate Intelligence Committee hearings.

Prior Writing Experience

A decade of experience working for software startups. Specialized in single-source cross-platform documentation, ranging from online help to API manuals. Wrote and edited thousands of pages; as team lead, was responsible for scheduling and mentoring new hires; advocated for usability testing and customer contact to meet reader's needs.

Professional Service

- Member of EPIC's Advisory Board (2014) [press release].
- Member of Center for Democracy & Technology's Academic Advisory Board (2014).
- Cookie Clearinghouse, Director (June 2013-present). The Cookie Clearinghouse provides information for users to make choices about online privacy. The Cookie Clearinghouse publishes free-to-use information for web browsers, users, and others [statement from Mozilla].
- World Wide Web Consortium (W3C), Tracking Protection Working Group, co-chair, 8/11 – 11/12. The Tracking Protection Working Group is chartered to improve user privacy and user control by defining

mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements. As co-chair, I focused on standardizing the meaning of Do Not Track. We worked on consensus decisions involving over 100 working group members from advertising/self-regulatory groups, corporations, browser makers, privacy advocates, and academics.

- California Office of Privacy Protection's Mobile Privacy Policy Advisory Group (2012).

Publications

Journal Publications

1. McDonald, A. M., and Lowenthal, T. Nano-Notice: Privacy Disclosure at a Mobile Scale. *Journal of Information Policy*, Vol. 3 (2013), pg. 331-354.
2. McDonald, A. M., and Cranor L. F. A Survey of the Use of Adobe Flash Local Share Objects to Respawn HTTP Cookies *Journal of Information Policy*, Vol. 7, Issue 3 (2011), pg. 639-687.
3. McDonald, A. M., and Cranor, L. F. Americans' Attitudes About Internet Behavioral Advertising Practices. *Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES)* October 4, 2010.
4. Leon, P. G., Cranor, L. F., McDonald, A. M., and McGuire, R. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. *Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES)* October 4, 2010. [CMU Tech Report]
5. McDonald, A. M., Reeder, R. W., Kelley, P. G., and Cranor, L. F. A Comparative Study of Online Privacy Policies and Formats. *Privacy Enhancing Technologies Symposium*, August 5-7 2009. [Author's version]

6. McDonald, A. and Cranor, L. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*. 2008 Privacy Year in Review issue. [Author's version]

7. Cranor, L., Egelman, S., Sheng, S., McDonald, A., and Chowdhury, A. P3P Deployment on Websites. *Electronic Commerce Research and Applications*, Vol. 7, Issue 3 (November 2008). Pages 274-293. [Author's version]

8. Reeder, R., Cranor, L., Kelly, P. and McDonald, A. A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. In *Proceedings of the Workshop on Privacy in the Electronic Society* (WPES 2008), Washington, DC, USA, October 2008.

9. James, R., Kim, W. T., McDonald, A. M., McGuire, R. A Usability Evaluation of a Home Monitoring System. SOUPS '07: *Proceedings of the 3rd Symposium on Usable Privacy and Security*. Pages 143-144, July 2007.

10. McDonald, A. M. and Cranor, L. F. How Technology Drives Vehicular Privacy. *I/S: A Journal of Law and Policy for the Information Society*, 2(3), Fall 2006, 981-1015. [Author's version]

Conference Proceedings

1. McDonald, A. M. User Perceptions of Online Advertising. *Yale ISP Conference* (March 25-26, 2011).

2. McDonald, A. M., and Peha, J. M. Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature. *39th Research Conference on Communication, Information and Internet Policy* (Telecommunications Policy Research Conference) September 25, 2011.

3. McDonald, A. M, and Cranor, L. F. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. *38th Research Conference on Communication, Information and Internet Policy* (Telecommunications Policy Research Conference) October 2, 2010.
4. McDonald, A. M. Cookie Confusion: Do Browser Interfaces Undermine Understanding? In *Proceedings of the 28th International Conference Extended Abstracts on Human Factors in Computing Systems* (2010). CHI EA '10. [Author's version]

Technical Reports

1. McDonald, A. M. and Cranor, L. F. A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies. [CMU Tech Report]
2. Leon, P. G., Cranor, L. F., McDonald, A. M., and McGuire, R. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. [CMU Tech Report]
3. McDonald, A. M., and Cranor, L. F. An Empirical Study of How People Perceive Online Behavioral Advertising. CyLab Technical Report 09-015. November 10, 2009. [CMU Tech Report]
4. Cranor, L. F., McDonald, A. M., Egelman, S. and Sheng, S. 2006 Privacy Policy Trends Report. CyLab Privacy Interest Group. January 31, 2007. [Author's version]

In Review

1. McDonald, A. M. When Self-Help Helps: User Adoption of Privacy Technologies. To appear in *Visions of Privacy in the Modern Age*, EPIC (2014).

2. Reidenberg, J., McDonald, A. M., Schaub, F., Sadeh, N., Acquisti, A., Breaux, T., Cranor, L. F., Liu, F., Grannis, A., Grey, J., Norton, T., Ramanath, R., Russell, N. C, Smith, N. A., Wilson, S. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. (Abstract submitted; manuscript in preparation.)
3. Grogan, S. and McDonald, A. M. Can I See Too? Contrasting Data Access and Correction in the United States and Europe.
4. McDonald, A. M. Browser Wars: A New Sequel? To appear in *The Journal on Telecommunications and High Technology Law (JTHTL)*, Vol. 11 (2013). [Slides from talk]

Related Non-Academic Publications

1. W3C Tracking Protection Working Group suite of documents (as a co-chair, I was primarily responsible for the Tracking Preference Expression Definitions and Compliance draft, but also contributed text to the Tracking Preference Expression draft, and commented on the Tracking Selection Lists draft) 2011-2013.
2. Mozilla Corporation, The Do Not Track Field Guide (co-authored with Sid Stamm; substantial input from Alex Fowler) 2011.
3. Mozilla Corporation, Online help for Do Not Track (authored the initial help files regarding Do Not Track shipped with Mozilla's Firefox browser) 2011.
4. McDonald, A. M. Position Paper for the W3C Do Not Track Workshop W3C Workshop on Web Tracking and User Privacy, Princeton, April 28-29, 2011.

Awards and Honors

Towards effective Web privacy notice and choice: a multi-disciplinary perspective. Team member of a multi-university NSF Secure and Trustworthy Cyberspace (SaTC) Frontier award. [NSF press release | Stanford press release]

CyLab Usable Privacy and Security Meritorious Achievement Certificate, 2010.

Barbara Lazarus Women@IT Fellowship, 2006-7. Received full tuition and stipend support for one year of doctoral scholarship.

Friedman Fellowship, summer 2005. Received support for a summer of technology policy work in Washington, DC.

Teaching Experience

Stanford University. ***Law-405, Privacy and Technology***, Spring 2013 Designed and co-taught with Jennifer Granick. Taught the legal basis for privacy, ways in which new technologies challenge existing legal and social frameworks, "notice and choice" and other theories for online privacy, how online advertising intersects with privacy, privacy enhancing technologies (PETS), privacy by design (PbD), and re-identification.

Carnegie Mellon University. ***Project manager. Policy Dimensions of New Space Technologies***, Spring, 2008. Responsible for a team of six undergraduate students as they defined, designed, and performed research regarding "new space" (entrepreneurial rather than NASA-led) business models, technologies, and federal policies. We submitted findings to our client, the Federal Aviation Agency. Created and graded quizzes. Contributed to assigning midterm and final grades.

Guest Lecturer

- Stanford University. M. Ryan Calo's law class, April 2012. Topic: Do Not Track.
- University of California, Berkeley. Deirdre K. Mulligan's Technology and Delegation, Fall 2011. Co-presented with Nick Doty. Topic: Do Not Track Overview.
- Carnegie Mellon University. Lorrie Faith Cranor's Usable Privacy and Technology, Fall, 2011. Topic: Do Not Track.
- Carnegie Mellon University. Lorrie Faith Cranor's Usable Privacy and Technology, Spring, 2008. Topic: Online privacy policies. Also led a class tour of a biometrics laboratory.
- Carnegie Mellon University. Lorrie Faith Cranor's Usable Privacy and Technology, Spring, 2007. Topic: Visualizing privacy
- Carnegie Mellon University. Lorrie Faith Cranor's Privacy Policy, Law, and Technology, Fall, 2007. Topic: Privacy policies and privacy communication.

Editorial Experience

- Program Committee, Hot Topics in Privacy Enhancing Technologies (HotPETs), 2014.
- Program Committee, ASE International Conference on Privacy, Security, Risk and Trust (PASSAT), 2014.
- Reviewer, Journal of Information Policy (JIP), 2014.
- Program Committee, IEEE Web 2.0 Security and Privacy, (W2SP), 2014.
- Program Committee, Workshop on Privacy in the Electronic Society (WPES), 2012.

- Program Committee, Privacy Enhancing Technologies Symposium (PETS), 2011.
- Reviewer, Information Systems Frontiers, 2010.
- Program Committee, Privacy Enhancing Technologies Symposium (PETS), 2010.

Presentations

Policy

Do Not Track briefings and progress updates. While co-chair of the W3C Tracking Protection Working Group, I conducted outreach to keep policy makers informed. From September, 2011 to June, 2013 I held approximately two dozen meetings and spoke with members of Congress and their staff members, European policy makers at the DG INFSO, as well as policy makers within the NTIA, Commerce Department, and White House.

Testimony before the California Assembly Select Committee on Privacy. Privacy Implications of the New Mobile App Ecosystem. March 26, 2013.

Testimony before the California Assembly Judiciary Committee, the Assembly Business, Professions and Consumer Protection Committee, and the Assembly Select Committee on Privacy. Balancing Privacy and Opportunity in the Internet Age. December 12, 2013.

Supported Alex Fowler's testimony to the US Senate Commerce Committee Hearing on Do Not Track, June 27, 2012.

Discussion with the California Attorneys General Consumer Protection Lawyers. Organized by Chris Hoofnagle, University of California at Berkeley. December 14, 2011.

Joseph Wender, Legislative Director for US Representative Ed Markey. Briefing on privacy technologies. October 18, 2011.

FTC staff regarding mobile privacy research. March 20, 2012.

FTC Commissioner Brill and staff. Preview of research findings on user expectations for Do Not Track. July 13, 2011.

Federal Trade Commission staff. Preview of research findings on user expectations for Do Not Track. June 15, 2011.

Federal Trade Commission staff. Beliefs and Behaviors: Internet Users' Understanding of Targeted Advertising. October 13, 2010.

Supported Lorrie Faith Cranor's panel discussion on consumer privacy expectations at the Federal Trade Commission's first privacy round table, December 7, 2009.

Supported a portion of Lorrie Faith Cranor's testimony to the Federal Trade Commission Ehavioral Advertising: Tracking, Targeting, & Technology town hall meeting, November 2, 2007.

Invited Talks

- World Affairs Council. The Internet of Things: Ubiquity Fueled by Innovation (moderator). May 7, 2014.
- Stanford Technology Law Review Symposium. CalOPPA panel regarding the "Do Not Track" provisions of AB 370 (moderator). April 11, 2014.
- American Bar Association. Video Games and Big Data: The More You Play, the More Others Learn, Ethical Obligations. March 17, 2014.

- Stanford Parents' Weekend. Internet Privacy: Policies and Practices. February 22, 2014.
- University of Amsterdam Institute for Information Law (IViR) and University of California, Berkeley School of Law. Workshop on Browsers and Tracking Protection. February 12, 2014.
- Stanford Political Science department. Regulatory challenges and privacy issues associated with mobile technologies. January 17, 2014.
- Stanford Institute for Economic Policy Research. Big Data, Big Issues. October 25, 2013.
- University of California, Berkeley. TRUST security seminar. September 26, 2013.
- Microsoft (LCA Speaker Series). The Cookie Clearinghouse. September 17, 2013.
- Privacy Identity Innovation (PII). Data Collection and Consent: Next Steps for Digital Advertising. September 16, 2013.
- Terms and Conditional May Apply. Discussion following local movie premier, August 3, 2013.
- AdMonsters. Cookie Clearinghouse. July 10, 2013.
- IAPP Summit. The Status of Do Not Track. March, 2013.
- Public Policy Students Colloquium. Internet Privacy: Policies and Practices. April 9, 2014.
- USC Annenberg Innovation Summit 2013 (discussant). April 4, 2013.
- Mobile 2.0. Mobile Security and Privacy and Trust - How Will Consumers Be Protected? September 11, 2012.

- Interactive Advertising Bureau (IAB) Town Hall. Do-Not-Track and Digital Advertising: What Happens Next? June 12, 2012.
- Future of Privacy Forum's App Privacy Summit (discussant). April 25, 2012.
- Microsoft (Online Services Division). December 8, 2011.
- Katholieke Universiteit Leuven. Do Not Track and US Privacy Bills. June 24, 2011.
- Institute for Information Law of the University of Amsterdam and the Berkeley Center for Law & Technology of the University of California School of Law. Online Tracking Protection Workshop. June 22-23, 2011.
- Online Tracking Protection & Browsers. Regulatory landscape: consent to be tracked? Panelist. June 22-23, 2011.
- Federated Social Web Europe, Following Social Advertising in the United States. June 3-5, 2011.
- Rapleaf 2011 Personalization Summit. Personalization and Privacy: A Birds Eye View. Panelist. May 26, 2011.
- Privacy Identity Innovation (PII) 2011. Panelist. May 18-21, 2011.
- W3C Workshop. Position paper for the W3C Do Not Track Workshop.
- Yale ISP, From Mad Men to Mad Bots. Discussion of the Psychology of Online Advertising. March 25-26, 2011.
- Admonsters Conference on Do Not Track. May 3, 2012.

- Microsoft. Beliefs and Behaviors: Internet Users' Understanding of Targeted Advertising. October 28, 2010.
- Carnegie Mellon Silicon Valley Talks on Computing Systems. August 11, 2010.
- Google Tech Talk. Privacy Targets: Three User Studies on Internet Privacy and Targeted Advertising. June 1, 2010.
- eMetrics panel discussion with Bob Page (Yahoo! Analytics) and John McKean (Center for Information Based Competition.) "The Great Cookie Debate or Your Personally Identifiable Information or Your Life!" October 22, 2009.
- Google Tech Talk. Online Privacy: Industry Self Regulation in Practice. September 17, 2009.

Conference Presentations

- University of Colorado. Silicon Flatirons. November 2, 2011.
- Symposium On Usable Privacy and Security (SOUPS). The Battle over the Behavioral Advertising Choice Mechanisms. Panelist. July 22, 2011
- 9th Workshop on Privacy in the Electronic Society (WPES). Americans' Attitudes About Internet Behavioral Advertising Practices, with L. F. Cranor. October 4, 2010.
- 38th Research Conference on Communication, Information and Internet Policy (TPRC). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, with L. F. Cranor. October 2, 2010.
- Privacy Law Scholars Conference (PLSC). Impressions and Privacy: A study of American Internet Us-

ers' Attitudes about Targeted Advertising, with L. F. Cranor. June 3, 2010.

- Privacy Enhancing Technologies Symposium. A comparative study of online privacy policies and formats, with R. Reeder, P. G. Kelley, and L. F. Cranor. August 5-7 2009.
- The 36th Research Conference on Communication, Information and Internet Policy (TPRC). The Cost of Reading Privacy Policies, with L. Cranor. Sep 27, 2008.

Media Coverage

Interviews regarding privacy with CBS, NBC, NPR, The Washington Post, The New York Times, Time Magazine, Tech Republic, The Register, ComputerWorld, Bloomberg BNA, Adweek, Ad Age, Business Insider, Politico, The Atlantic, and many others.

Do Not Track efforts generated thousands of articles, few of which I contributed to. Coverage of research regarding user expectations of Do Not Track:

- Davis, Wendy. Study: Consumers Define Do-Not-Track More Broadly Than Web Companies. ***The Online Daily Examiner***. (3 May, 2011)
- Tarran, Brian. Do-not-track isn't just about advertising, say web users. ***Research***. (4 May, 2011)

Coverage of LSO ("Flash cookie") study:

- Davis, Wendy. Have Web Sites Cut Back On Flash Cookies? ***Daily Online Examiner***. (31 Jan, 2011)
- Mullen, Joe. New Study Shows Persistence Of 'Flash Cookies' ***Paid Content***. (1 Feb, 2011)
- Tarran, Brian. Flash cookie respawning 'on the wane', say Carnegie Mellon researchers. ***Research***. (3 Feb, 2011)

Coverage of errors in P3P compact policies:

- Davis, Wendy. Privacy Snafu As Web Sites Bypass Cookie-Blockers. ***Daily Online Examiner***. (10 Sep, 2010)
- Dissent. Is your browser being lied to? Survey says: "Maybe". ***PogoWasRight***. (13 Sep, 2010)
- Marc. Cookie Control. ***p2pnet news***. (13 Sep, 2010)
- Marc. Cookie Control: Part II. ***p2pnet news***. (14 Sep, 2010)
- Maier, Fran. Let's talk P3P. TRUSTe. (13 Sep, 2010)
- Richmond, Riva. A Loophole Big Enough for a Cookie to Fit Through. ***The New York Times***. (17 Sep, 2010)
- Tarran, Brian. Oh crumbs! Cookies left unblocked by code errors, say academics. ***Research-Live***. (13 Sep, 2010)

P3P compact policies enforcement actions:

- *Del Vecchio et al* v. *Amazon.com* class action filing
- Eaton, Nick. Suit: Amazon fraudulently collects, shares users' personal info. ***Seattle PI***. (3 Mar, 2011.)
- Enright, Allison. Privacy suit takes aim at Amazon. ***Internet Retailer***. (4 Mar, 2011.)

Coverage of mental models of online advertising and behavioral targeting:

- Davis, Wendy. Study: Consumers Equate BT With 'Privacy Harm' ***Daily Online Examiner***. (17 Nov, 2009)
- Kessler, Sarah. Online Behavior Tracking and Privacy: 7 Worst Case Scenarios. ***Mashable***. (3 Nov, 2010)

- Trager, Louis. Privacy Desires Unmet: User Ignorance, Assumptions Undermine Targeted Ad Self-Regulation, Say Researchers. *Communications Daily*. (11 August, 2010) [CommDaily is only available to subscribers]

Our findings about the value of the time required to read privacy policies were covered by technology and legal publications, and blogged internationally in multiple languages. Highlights:

- Radio interview with Free Press on The Cost of Reading Privacy Policies (17 Oct, 2008)
- Anderson, Nate. Study: Reading online privacy policies could cost $365 billion a year. ***Ars Technica***. (8 Oct 2008)
- Davis, Wendy. Online Execs Object To Privacy Statement Report. ***MediaPost's Online Media Daily***. (9 Oct 2008)
- McGee, Matthew. Average privacy policy takes 10 minutes to read, research finds ***OUT-LAW News***. (6 Oct 2008)
- ***Slashdot***, 20 Hours a Month Reading Privacy Policies (10 Oct 2008)
- Whoriskey, Peter. Lost in the Fine Print: It Would Take a Week to Read All Your Privacy Policies. ***Washington Post I.T.*** (26 Sept 2008)
- Wilson, Tim. Users, Enterprises Pay for Poor Privacy Policies, Study Says. ***Dark Reading***. (7 Oct 2008)

ELAINE ADOLFO

January 2011-Current
Associate Director - Stanford Center for Internet and Society

Working within CIS, the Associate Director for CIS reports to the Faculty Director and is responsible for managing the operations of CIS including developing and implementing effective strategies to enhance the online presence of CIS through the web, social media or traditional print media, supervising center administrative staff, directly supporting the Faculty Director, and managing the finances and events for the center.

Develop and implement an effective web strategy for CIS

Manage re-design of CIS website, from the initial specification, calls for proposal to the actual re-design and content migration.

Proactively plan and track new content and ongoing updates. Execute updates and changes on schedule. Create and manage schedules for content additions and changes (including text, photo, and other web assets) and communicate project delivery plan and timelines to all project stakeholders.

Create content culled from the Faculty Director and the Fellows for distribution on their blogs, the CIS webpages in the SLS website, and all major social media outlets (Facebook, Twitter, etc). This involves digital communication of upcoming events, books, publications and or personal blog posts that benefits the reputation of CIS.

Prepare/format final content in web file formats.

Produce wire-frames, screen designs, webpage graphics, and other final assets such as final page designs, HTML, and color-corrected photos and graphics, optimized for

the web based on the sites' overall design guidelines, usability standards, and template protocols-to fulfill faculty director's and fellows' requests.

Supervise the work of students and outside consultants or contractors, such as Drupal consultants or front-end web developers.

Develop and implement an effective social media strategy for CIS.

Create and manage the CIS Facebook account and provide ongoing support. This involves cross promoting events placed in the blog into Facebook, adding events, dealing with users' comments and notifying the faculty director and fellows of any issues or topics raised in Facebook that might be of interest.

Create and manage the CIS Twitter account. Perform daily monitoring and raise issues or topics raised in Twitter that might be of interest to the faculty director and the fellows.

Be informed of the latest projects by the faculty director and the fellows and recommend ways their work can be promoted in the social space. Recommend and implement search engine optimization for these materials.

Provide ongoing support for the faculty director and the Fellows with all mass email communications to the public. This involves updates to newsletters and email blasts promoting an event or publication related to CIS. Monitor statistics of success of these different tools of communication and make assessment on future distributions.

Manage the production of and provide graphic design support for print media (i.e. CIS working papers & white papers and an annual report to be used at a variety of public venues)

Work with outside designers on various printed pieces. Coordinate with outside print houses for bids, specs, paper samples, and schedules.

Provide graphics support to the faculty director, including creation of content and graphics for other uses including: color corrected digital photos for print collateral, graphics for PowerPoint presentations, and the creation of PDFs for electronic distribution.

Provide direct support to the Faculty Director including travel planning, correspondence, calendar management, managing accounts receivable issues, and communications.

Manage the faculty director's literature database.

Coordinate and manage the Faculty Director's research assistants.

Manage the finances for the center including tracking and managing the budget, reimbursements for the center, and all financial reporting.

With the Law School Program Group, plan and execute all events for CIS including conferences, workshops and the speaker series.

Manage the administrative staff for the center including one administrative associate, interns, and research assistants.

Manage the recruiting process for center hires including fellows and support staff. Work with the faculty director to anticipate staffing needs.

Represent CIS within the law school, for example at meetings of the directors of the various centers.

June 2009-December 2010
Web Designer/Content Manger for the Communications Department at Stanford Law School
Design, manage and maintain content on all aspects of the law school's website. Update content through the CMS and with HTML updates. Design graphics including iconography and photographs. Create a variety of print materials from admissions brochures, faculty scholarship viewbooks and the annual photo directory. Manage student workers and train department colleagues on the use of blogs, social media tools and other online media.

2004-2009
Assistant to Lawrence Lessig at Stanford Law School
Primary duties consisted of managing Professor Lessig's schedule. This involved daily tracking of his schedule, managing appointments, building complex travel plans, and managing research assistants for 2-3 classes per semester. Managed and monitored Lessig's website Lessig.org. Cleared spam and inappropriate comments in his blog. Helped colleagues in the many groups he was affiliated. This involved administrative tasks and web tasks. Managed and implemented events on the Stanford campus and around the world.

2003-2004
Administrative Assistant for Residential Education at Stanford University
Assisted with the RA process for undergraduates. Created training materials for RAs while also planning events for student groups.

2002-2003
Producer - Apple Computer
Managed and produced the .Mac website for Apple Computer. This involved working with engineering, design and marketing groups to implement new designs on a daily basis. Worked with international teams to implement site changes and managed the schedule for translations with outside contractors at international locations. Produced launch campaigns from the point of creation, development, coding, launch and Q&A. Implemented designs for both web projects and presentations to senior staff.

2000-2002
Producer for the Tools Business Unit - Macromedia
Managed production team and produced the launch of three product launches. Developed mockups and editorial schedule for online promotions and tutorials. Worked with product management in planning online designs that met with business goals. Worked with engineering on creating key applications that optimized customer experience and saved money for the company. Organized production schedules of freelance production artists and engineers. Analyzed site activity using Netline and provided suggestions based on statistical results.
Coordinated production efforts with an international production team. All content was translated in 10 languages for a simultaneous launch.

Education:
1998 University of California at Berkeley
Major: English Literature with emphasis on Modernist Literature

Amanda Avila

Administrative Associate

Stanford Law School, Center for Internet and Society

10/06 – Present

- Assist in building and maintaining the CIS digital community through the CIS website and CIS' social media channels. This includes daily content updates to our website that range from cross-posting blog posts, embedding new videos, adding new publications, creating photo albums, tracking all CIS Affiliates activities, and more as CIS content develops. Basic HTML knowledge and intermediate knowledge of social media tools is required for this role.
- Draft content used to engage constituents and grow channels. Curate digital content from Google Alerts and input from our CIS Affiliates. Implement social listening efforts and report back to Associate Director on issues needing special attention.
- Prepare email campaigns for distribution to our CIS mailing list and the Stanford community.
- Assist with travel arrangements for CIS staff.
- Plan and schedule conferences, meetings, and special events based on input from the Associate Director. Coordinate all aspects of these events from sending out email campaigns, booking vendors, and processing reimbursements payments.
- Purchase office supplies, order phones and office equipment. Responsible for setting up maintenance agreements on equipment and other vendor agreements.

- Reconcile ORACLE invoices with payments. Prepare reimbursements and allocate expenses to the correct accounts
- Other general clerical assistance including greeting visitors, distributing mail and faxes, answering telephones, photocopying, sending and receiving packages.
- Custodian for the division pcard and travel card. Verify expenses and clear transactions to the correct account, following university, department and IRS policies.
- Maintain up-to-date various distribution lists.
- Prepare legal documents with guidance from Directors.
- Prepare informational materials for CIS visitors and interns which include information about the resources available to them on campus to logistics at SLS.

Legal Assistant

Fonda & Fraser, LLP, Anaheim, California

10/02 – 9/06

- Handled wide variety of responsibilities in the support of a team of one senior and two associate attorneys to ensure the timely preparation of complex cases from discovery to trial phase. Responsible for filing court documents, providing necessary filing fees, retrieving documents from court when necessary.
- Maintained communication pipeline between attorneys, clients, healthcare providers, insurance carriers, law firms and government agencies. Drafted, transcribed, revised and finalized correspondence, pleadings and motions. Typing 75+ WPM.

- Extensive experience obtaining and gathering case-relevant data and materials through internet and law library research. Well versed in the use of Lexis and Westlaw research databases.
- Coordinated and maintained billing from vendors and experts for all cases, including closed and settled matters.
- Handled calendaring/scheduling of all appearances, meetings and depositions including coordination of travel, scheduling of court reporters, interpreters, and copy services.

APPENDIX G

[World Privacy Forum logo omitted]

May 4, 2014

World Privacy Forum Cy Pres Distribution Proposal

The World Privacy Forum[1] is pleased to submit a proposal for this online privacy-focused Cy Pres distribution. This proposal contains three parts, I: Overview; II: Proposal; III: Addendum.

The body of the proposal is 20 pages. An addendum includes additional biographical and publication summaries of WPF staff and experts, details and biographical summaries of the independent advisory board overseeing this grant, and a roster of recent WPF work, publications, testimony and lectures, and media reports.

I. Overview

Following is an overview of the proposal, deliverables, need for the work proposed, benefits to the class, and brief discussion of WPF's mission and purpose as an organization as well as our work and role in privacy.

A. Overview of Project Proposal and Deliverables

The World Privacy Forum is proposing two substantial projects for this Cy Pres distribution. The projects

---

[1] The World Privacy Forum is a non-profit public interest and consumer education research group. We are the only privacy-focused non-profit in the US that focuses solely on in-depth privacy research and consumer privacy education. The mission and purpose of our organization is to protect and advance consumer privacy in a digital era, particularly in the areas of technology, health care, finance, and the Internet, among other areas of privacy. WPF is based in San Diego, California, and has published many ground-breaking privacy studies of national and international interest, as well as consumer education. Please see <http://www.worldprivacyforum.org>.

are interrelated. The first project provides the research and factual foundation for the education and direct consumer support the second project provides.

The first project is a substantial research project that uncovers and brings to light third-party data flows and consumer harms stemming from consumers typing search queries into online search boxes, and submitting other information online through forms and other means. The research focuses on variety of types of web sites with search query boxes that can lead, and have led to, consumer harms. For example, medical-related, financial-related, data broker, "people finder," and other web sites often have search query boxes and online forms tied to third party data flows, which may be difficult for consumers to detect. This project has a significant research component, substantial deliverables, and a consumer education component.

This project meets the requirements of the cy pres by uncovering and documenting third party data flows online, documenting specific online consumer privacy harms, educating and protecting consumers and the cy pres class about and from the online harms in the project area, providing direct support to consumers who have experienced privacy problems and need assistance, informing policy makers about risks to consumers and the cy pres class members by disclosing their information to ISPs and websites, by suggesting solutions, and by establishing a fact pattern to support effective, positive change for consumer privacy.

Deliverables for the first project include:

- Three substantive research reports (medical focus, financial focus, databroker and peoplefinder focus) These three reports will uncover, factually document, and shed light on third party data flows, activities at

these sites using information typed into search query fields and other online forms, consumer harms arising from documented practices, and make corrective policy recommendations and solutions based on the findings.

- One consumer-focused report on online privacy based on the research and the results. This report will be written and designed specifically for consumers, including what to do, solutions regarding risks of disclosing information to ISPs and web sites, specific advice and tips for specific types of sites, and general privacy tips, inclusive of search engine tips and other online privacy tips. The report will be structured in a way that allows maximum readability and accessibility.
- 4 free-to-consumers ebooks.
- 3 consumer education videos. These videos will highlight for consumers the risks they face when they disclose information to third parties online, and give consumers solutions, tips, and practical work-arounds for using technology in a way that is also privacy-protective.
- Digital brochures (one pagers, wallet cards summarizing consumer tips and information).
- Curriculum materials for teachers and educators focused on the three types of web sites researched. These materials will assist teachers of grades 6-12 to educate younger class members on risks of disclosure and solutions.
- Half-day conference to disseminate findings of project research, curriculum, and research and educational materials to teachers, educators, community leaders, policy makers, and NGOs. The materials for

this workshop will be specifically tied to this research and the consumer advice and information established by the fact patterns uncovered and documented in the research.

The second project is a national consumer education project focused on bringing online privacy education to all consumers, with a particular focus on vulnerable consumers who often miss online privacy educational campaigns due to financial, linguistic, educational, medical, or other barriers. This project will create and deliver online privacy training customized to vulnerable consumers, in a way that is meets their needs in order to facilitate effective communication and help.

While the first project has its own broad consumer communication component, the second project will take the research material and hone it and refine it for communicating specifically for key vulnerable consumer populations and consumers and cy pres class members affected by the harms uncovered by the research, but the least likely to be reached by traditional, broadly focused education campaigns.

Deliverables for the second project include:

- Direct consumer support for duration of grant (3 years): support for consumer queries about online privacy via email and phone.
- Direct consumer outreach. (workshops, free-to-consumer training sessions both online and off, and other direct to consumer outreach.)
- Robust consumer privacy education materials (based on cy pres research) specifically tailored for the following groups:
    - Teens
    - Seniors

- Financially vulnerable
- Victims of crime
- Individuals with medical or other challenges including disability
- Underserved populations
- Spanish speakers

- Consumer materials will be published online, and some materials will also be printed for delivery to consumers who require or strongly prefer print delivery. Materials include
  - Tipsheets and focused consumer guides (tailored to audience)
  - One-pagers (tailored to audience)
  - Wallet cards (tailored to audience)
- 8 instructional videos (tailored to audience)
- Training curriculum (One training curriculum containing information about consumer education for vulnerable populations, with specifics for each group. The curriculum is intended to be used as an adjunct to the curriculum developed in Project One and is intended to be used by both educators, community leaders, NGOs, and other individuals working directly with vulnerable populations.)

Both projects are designed to meet significant consumer privacy knowledge and educational needs, to document third party data flows, the support consumers directly, and to create materials that will provide research and information that will factually document online consumer privacy harms, and by so doing allow policy makers to better see and understand the issues and assist this class of consumers. The project will provide tools

and techniques to assist consumers in solving online privacy problems.

To ensure transparency, timely deliverables, and accountability for these projects, WPF has convened an advisory board to oversee the implementation of the proposed projects.

B. How these Projects Address, Serve, and Benefit the Class

The proposed projects and resulting deliverables address, serve and benefit the class members by:

- Providing research about third party data flows in regards to information consumers submit to online web sites via search query boxes or online forms.
- Educating the class members, including vulnerable class members, about the risks associated and documented regarding disclosure of information to third parties online, including ISPs and websites.
- Providing information and solutions to policy makers regarding online privacy and third party data flows impacting consumers.
- Providing consumer education in multiple formats (print, video, online) that assist consumers in understanding privacy impacts, risks, and potential harms and provide workarounds and tools for avoiding privacy harms.
- Providing direct consumer support and tools/workarounds for consumers who need direct assistance with online privacy questions and concerns.

C. Transparency and Oversight

WPF will be reporting the results of research, consumer education, curriculum materials, and trainings and will be creating numerous published materials as a result

of this cy pres. The research, consumer, and educational material will be made publicly available free of charge, and will be widely disseminated. WPF will be reporting on the progress of the grant on its web site at regular intervals.

Additionally, we have convened an independent advisory board specifically to provide oversight for this cy pres and the related proposals. WPF will regularly report to the advisory board and consult with them about project deliverables, budget, and implementation.

D. Overview of WPF's Work

Our mission and purpose is aligned completely with the goals of the settlement. The mission and work of the World Privacy Forum is to protect consumer privacy in a digital era and to create the tools and knowledge consumers need to shape and control their information and their digital lives.

WPF is a public interest research and consumer education group focusing exclusively on consumer privacy, in particular, digital privacy. We are the only privacy-focused public interest research group in the US, and we have built up a large body of research, consumer outreach, and accomplishments in the area of consumer privacy and digital and online privacy in various topic areas. Our organizational mission and goals completely revolve around consumer privacy, and all of our operations and projects do as well.

We have a strong and well-earned reputation for work of the highest caliber that is also impactful and groundbreaking. Our work informs policymakers and consumers of risks and solutions with deeply researched materials that often break new ground. For example, two of our recent reports, *The Scoring of America: How Secret*

Consumer Scores Threaten Your Privacy and Your Future, (April 2014) and Data Brokers and the Federal Government, (October 2013)—reports that are original in their research and bring new information to the public—were cited by the White House in its most recent privacy report on Big Data (May 2014), and our most important recommendations to enhance consumer privacy in the area of big data and data brokers were adopted in the White House report. WPF was also asked to discuss the *Scoring of America* research material at an FTC workshop on predictive analytics regarding impacts and risks to consumers.

Our work also impacts consumer privacy at the ground level. For example, our consumer privacy work has directly resulted in new consumer protection laws of significance. Our Medical Identity Theft report, which identified, documented, and discussed medical identity theft for the first time (*Medical Identity Theft: The Information Crime that Can Kill You*, 2006) included recommendations that directly resulted in the California medical data breach statute, which then influenced a change in the Federal HIPAA regulations to include a requirement to inform consumers of medical data breaches. Today, medical identity theft is a well-known and acknowledged consumer issue that many stakeholders, including the US government, are working on. Medical data breach statutes are now seen as commonplace, but prior to our report, this was not the case.

WPF was a key part of the lead drafting team that successfully brought to completion a new national-level mobile application short form privacy notice as part of the US Department of Commerce NTIA Multi-Stakeholder Process (2012-2013). Our recommendations to expand the definition of medical privacy and to include

data brokers in the notice were accepted, as was our recommendation to ensure privacy notices were consistently available from apps on mobile devices.

Earlier, WPF crafted the Do Not Track proposal and language, and brought that issue forward for the first time (2008). The Do Not Track issue has received global attention and a great deal of national policy work. Our work also educates consumers directly on privacy issues. We maintain and update key consumer privacy resources, unique in their depth and usability, such as the Patient's Guide to HIPAA, Data Broker Opt Out List, Top Ten Opt Out List, Medical ID Theft FAQ for Victims, and many other resources. Two members of WPF's team co-authored a reference book on online privacy that was published in 2011. (*Online Privacy*, Robert Gellman and Pam Dixon, ABC-CLIO).

WPF has testified on the issue of consumer privacy protection before Congress multiple times, most recently in December 2013 on data brokers, in 2011 about consumer expectation of privacy both online and offline, and in 2009 about online privacy, the modern permanent record, and consumers. WPF has also testified before the FTC, FDA, and other federal agencies many times on the topic of consumer privacy. Our reports and our work receive consistent, substantial press coverage, and have for many years.

Topics we have engaged with include: Search engine privacy, online privacy, ad privacy, mobile privacy, employment and online job search privacy, data brokers, online background checks, social media privacy, communications privacy, financial privacy (including online), opt out, self-regulation and privacy, health privacy, identity theft, medical identity theft, genetic privacy, biometrics and privacy including digital signage networks and retail

privacy, privacy and big data, privacy and vulnerable populations, privacy and sensitive information, privacy and victims of crimes and domestic violence, among other consumer-focused privacy topics.

II. Proposal

We are proposing two interrelated projects; the first project provides significant privacy research and education that supports the cy pres goals and cy pres class members, the second project provides a national education campaign and direct consumer support based on the facts established by the research that supports the cy pres goals and cy pres class members. The second project tailors education and consumer support materials for vulnerable populations in addition to the general consumer education campaign.

A. Project One: Research and consumer education around online search boxes, forms, and referral headers that lead to privacy mischief (For example, data brokers, people finders, loan application sites, medical-related search boxes, and other online search boxes.)

Consumers who type in queries and fill in a variety of forms online may have their information sold, disclosed, and used in ways that are unexpected and potentially harmful. This area is where a great deal of privacy mischief and outright consumer harm is occurring.

Consumers typically begin their web browsing with a search box of some sort, and then continue typing in queries across web site search boxes as they read information, shop, communicate, and explore. Unknown to many if not most consumers who are actively typing in search queries, a significant number of search boxes online lead back to online data brokers and their many affiliates. Some search boxes for online financial and loan

sites lead to scammers and identity thieves. Some of the information, when it is disclosed to third parties, puts financially vulnerable consumers on lists of people who are living in or near the poverty line, information which then can be sold. Some search boxes and registration forms on medical-related sites lead to third-party data flows that allow consumers' information to be shared on data broker lists. There are many other examples. Some unseen third-party data flows have been documented, for example, WPF has documented some of these issues in our work on data brokers including Congressional testimony and two recent reports. There are, however, an astounding variety of these types of challenging search boxes online, and many of the most important ones are still under-researched, and under-documented online.

This proposed project meets the need for research and factual information and insight about solutions for the cy pres class in this areas. This project specifically investigates and illuminates this issue of consumer risk related to disclosure online via search boxes and forms, providing factual information for policymakers and key information and advice for consumers. This project meets the needs of the class members by providing vital research, consumer education, outreach, and support in this critical area. It also meets the needs of the class by providing critical information to policymakers on this issue about solutions, based in actual fact. It also provides information about third party data flows.

WPF is the leading privacy group in the area of online privacy and data brokers, and is uniquely positioned to conduct this project successfully. We have already conducted a great deal of research related to this topic, and are well-situated in expertise, experience, and focus to undertake this project and complete it successfully.

This project will create three in-depth research reports about the hidden data flows occurring behind data broker sites, online people finders, consumer list brokers, online loan application sites, medical web sites, and other key areas where consumers type in sensitive information. The reports will tease out the facts and details of these sites, which have not been heretofore documented. The project will also fund a very significant national consumer education campaign around the report findings, with online and offline education that includes education through multiple channels, including video, direct consumer support and education, e-books, workshops, and a variety of online materials.

1. Project goals and description

A key goal of this project is to uncover, document, and bring transparency to the data privacy practices and third party data flows of a variety of web sites in key areas that are of critical importance to consumers, but are either under- or undocumented. Consumers who give their information to sites via search queries or other means often do not see or know about the back-end or secondary uses of their submitted data, particularly in regards to data broker activity, which is highly personal to consumers, and has marketplace impacts. For example, our recent Scoring of America report uncovered and documented that consumers who reveal certain diseases online, some of them doing so by simply filling out a form for more information, may have that information used in unexpected ways—such as setting a price for their health plan premium.

We have identified three key areas to research that are of key concern for consumers, and pose high risk for consumer harm, that is, risks of disclosures and third party data flows at:

- Data brokers, broker-related "people finder" web sites, and online consumer list brokers.
- Medical-related web sites.
- Financial-related web sites.

By focusing on the sites with the highest harm risk to consumers, we have the opportunity to uncover unique harms, risks, and solutions associated with each type of site. Our work has taught us that the risks for all web site types is not identical.

A second goal of this project is to provide information to consumers so they can make informed and effective choices about their risks when presented with a search box online or a form to fill in. There are an astounding variety of these types of boxes and forms, and consumers have little material about potential consequences or effective work-arounds, or how to identify when risk is present. To meet this goal, WPF will write a robust consumer guide based on the factual information uncovered in the research. The guide will be written for consumers in a digestible format and will expose and discuss this information specifically for consumers.

The research component of this project allows WPF to ground-truth and factually document actual online practices, including referral header practices from search boxes across a wide swath of the Web. The consumer education and outreach component will allow us to distill our knowledge and engage with the class members to assist them with the very real problems and challenges posed by using these kinds of search boxes and information tools online.

WPF has been engaged for the past year and a half in a groundbreaking research project on data brokers. We have published two major reports with our findings, with

a third to come. These reports have documented two aspects so far of fundamental data broker privacy issues and understanding the operations of data brokers (government use of data brokers, predictive analytics and data brokers). Along the way in our current research, we have learned some things that we did not expect, and the information has direct bearing on this proposal and these class members.

For example, the symbiosis of online data broker activities with aggressive affiliate programs and other activities that use aggressive and often hidden to the consumer referrer-header techniques from search boxes—among other techniques—to capture unwary consumers and consumer information online, is widespread. Consumers are routinely captured from multiple compelling search boxes across the Internet. There is not enough consumer-focused, sector-specific documentation of this, there is not enough consumer education around this, and there is almost no consumer education on this topic dedicated to serving the vulnerable consumer populations that need the information the most.

2. Project Deliverables:

This proposed project will fund three in-depth research reports about data brokers, online people finders, and consumer list brokers and the specific online and policy issues related to their activities relating to consumers. The reports will tease out the facts and details of these sites.

These reports serve the class precisely, because they deal directly with the class who is typing search queries into search engines and search boxes. The research is complex, and we know from our current project that three focused reports in three areas are the correct research approach to documenting this issue.

The other component this project would create is a full consumer guide based on the research, which would form the basis of an education campaign online and [illegible] about data-broker fueled people finders, list brokers, and a wide range of other data broker activities online. WPF has a good understanding of the educational necessity of reaching out to all segments of the class who can be impacted by these data broker activities, including all members of the class from those with a great deal of knowledge to vulnerable populations such as seniors and teens and disabled individuals who are often directly targeted by bad actors using sophisticated technologies as these consumers search for help or just other people or even information about themselves online. No such materials exist at this time. Note: Digital materials created for this project will be mobile-compatible.

Full list of deliverables for Project One includes:

- Three substantive research reports (medical focus, financial focus, databroker and peoplefinder focus) These three reports will uncover, factually document, and shed light on third party data flows, activities at these sites using information typed into search query fields and other online forms, consumer harms arising from documented practices, and make corrective policy recommendations based on the findings.
- One consumer-focused report on online privacy (This report will be written and designed specifically for consumers, including what to do, specific advice and tips for specific types of sites, and general privacy tips, inclusive of search engine tips and other online privacy tips. The report will be structured in a way that allows maximum readability and accessibility.)
- 4 free-to-consumers ebooks (This will make the three reports and the consumer guide available across mul-

tiple platforms to increase availability to consumers and to policy makers.)

- 3-4 consumer education videos (Each video briefly discusses an aspect of the consumer tips resulting from the research.)
- Digital brochures (one pagers, wallet cards summarizing consumer tips and information based on the research)
- Curriculum materials for teachers and educators focused on the three types of web sites researched
- Half-day online privacy conference to disseminate findings of research, curriculum, and research and educational materials to teachers, educators, community leaders, policy makers, and NGOs. The materials for this workshop will be specifically tied to this research and the consumer advice and information established by the fact patterns uncovered and documented in the research.

3. Why this project is needed

Search boxes abound online. Most consumers begin their web browsing with a search box of some sort, and then continue typing in queries across web site search boxes as they read information, shop, communicate, and explore. Unknown to many consumers, a significant number of search boxes lead back to online data brokers and their many affiliates. Consumers who search out medical or financial information would be surprised to learn the third party data flows impacting where their information goes and how it is ultimately used. This is where a great deal of privacy mischief is occurring.

Consumer understanding of and factual information about data brokers and their operations online is a significantly under-researched area. As a result, consumer

outreach and education in this area is similarly lacking. These gaps are due in large part to the difficulties of conducting meaningful, robust research in this area. It takes excellent depth of privacy expertise, technical expertise, policy expertise, and it also takes an in-depth knowledge of the data broker system. The combination of this skill set is quite rare. Meanwhile, in the absence of transparency and a sufficient factual knowledge base, substantial numbers of data brokers and shady, aggressive affiliate operations are causing great harm and suffering to consumers, in particular, this cy pres class.

These research and consumer education materials do not exist at this time. The World Privacy Forum is the organization with the most knowledge of data brokers, medical privacy, and other online privacy activities in the United States today. Combined with our privacy and technical and education skills, we are among the most qualified organization in the US to do this work, if not the most. WPF already has an experienced and proven research and education team in place to execute this project nationally. We have written several FTC data broker complaints that have resulted in FTC investigations and subsequent enforcement actions in this area already. If we are funding for both of our large proposed projects, we will be able to take this research and deliver consumer materials to a wide variety of class members, including those who are hard to reach. (See Project One in this proposal.)

4. Project Requirements

To complete this three-year project we will need $540,000 total for staffing and materials to research the reports, write the reports, fact check the reports, edit and proof the reports, and create the final content deliv-

erables. The project will be budgeted at approximately $180,000 a year, paid over three years.

We will also use the funding to distill the report information into high-quality consumer tips, guides, one-sheeters, wallet cards, and educational videos. We test the consumer-focused content with class members, create a national rollout and distribution plan, and then execute that plan with the content.

Specifically, we will need the following materials and staff as discussed below to complete the project:

- **Research Component:** We will use our own personnel to conduct the research for the reports. The WPF specializes in research, and we have a great deal of experience in producing research of the highest caliber. We will use our proven team for this project, and we will use an independent qualified fact checking company for quality assurance.

  Personnel, Research Component:

  - Research – lead investigator (Pam Dixon)
  - Research – research assistant (Marianne Fitzpatrick, staff)
  - Research – legal analysis (Robert Gellman)
  - Research – fact checking (First pass, staff. Second pass review, including technical review, outsourced for quality control.)

- **Consumer material writing, editing, posting, maintenance:** We will primarily use our own personnel to write, test, and finalize the consumer-facing content resulting from this project. (Please see organizational information for bios of our executive director and other collaborating experts for the writing/testing portion of this project.) We anticipate

substantive and ongoing consumer content. (See "Other Project Components below.)

Personnel, Consumer material writing, editing, posting, maintenance:

- Writing, editing: Pam Dixon, Bob Gellman, other staff.
- Final proofing: (First pass, staff, second pass, technical: outsourced)
- Maintenance and updating: WPF staff.

- **Consumer Education and Outreach/ Content distribution plan:** WPF staff will ensure the consumer education component is a robust part of the distribution, rollout, and consumer outreach. We will also confer with the independent project advisory board, which has education expertise.

  Personnel, Consumer Education and Outreach project staff:

  - Consumer education director: The WPF consumer education director will be responsible for rolling out and executing the outreach segment of this project, which will include online and offline components.
  - Consumer education assistance and outreach: Staff
  - Project Oversight: Executive director, independent advisory board.

- **Web and data visualization:** We will work with John Emerson to create the web pages and the visual components of the materials. (Please see organizational information for biographical summary.)
- **Video education component:** For this project, we will create educational videos for consumers and how-

to videos for specific search query issues. We plan for the project to require approximately 3 consumer education videos. WPF staff will complete the video components.

Additional Project Components:

- **Digital and print brochures, one-pagers, and wallet cards:** We will create digital materials that can be repurposed across many mediums, including paper. All materials will be distributed online, and we will give people the ability to further print out the materials via our site. (This would function very similarly to the FTC's consumer education print outs; see <http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html>.)
- **Curriculum materials for teachers and educators in key outreach environments:** WPF will extend the impact of this project by creating and delivering materials to individuals who can reach further into the community of class members. We will craft curriculum materials to assist with this.
- **Half-Day Privacy Training Conference:** After the research has been completed, we will host a half-day conference to convene privacy groups, consumer groups, industry stakeholders, government stakeholders, and other relevant stakeholders to discuss the issues raised in the research and to disseminate training materials. The focus will be on sharing knowledge and finding practical and policy solutions for consumers and developing a coalition of groups to continue further work on the consumer privacy issues raised in the research, as well as encouraging a public dialogue.

5. Project Budget

The project budget is 540,000 (over three years) or 180,000 per year.

Expenses:

Personnel

Research (4 reports, teaching curriculum) (legal, technical, and policy research): $300,000

Review and Fact Check (4 reports, teaching curriculum) (Full review, including technical review of research): $25,000

Writing (4 reports, consumer materials, curriculum materials): $100,000

Video/Filming/Editing/Final preparation (3 videos): $7,000

Editing/Proofing (including line edit and final proofing of 4 reports, curriculum, consumer materials) $15,000

Web/report/ebook layout (website preparation of 4 reports, curriculum, report layout and formatting, ebook formatting, layout, and final preparation.): $25,000

Consumer Education/Outreach/Dissemination: (Specifically of Project One deliverables to a national consumer audience) $15,000

Infographic design for data flows and illustrations (illustrations will be used in reports, web, ebook, printed/digital materials for consumers): $10,000

One half-day conference to disseminate curriculum materials, train non-profits, community leaders, consumer advocates, and teachers: (personnel costs) $5,000

Other Project Expenses:

Operations and material costs directly associated with the proposed project. No separate or unrelated overhead costs are included.

Project ebook ISBN (ISBNs from Bowker to allow publication of 4 free consumer ebooks across several platforms) $2,000

Project Postage: $1,000

Project Printing: $5,000

Project Travel (Travel budget is to support project deliverables only): $5,000

Half-day training conference: This conference is expressly to disseminate curriculum materials, train nonprofits, community leaders, consumer advocates, and teachers. We will endeavor to find in-kind donations to host the conference and will seek to minimize funding going toward those operations. Any funds remaining will go toward direct consumer support. $25,000

B. Project Two: Online privacy and Internet search outreach and education for teens, seniors, and under-served, vulnerable individuals

This project creates consumer educational content around online privacy and disseminates it in multiple mediums for vulnerable cy pres class members and consumer populations nationally.

The educational content will facilitate communicating the findings of the research and consumer advice uncovered in Project One of this proposal, which is directly related to the cy pres needs. An important advancement this project brings is to develop a robust array of tailored, focused national consumer education campaigns

around online privacy specifically for a variety of vulnerable consumer populations.

The vulnerable population education and outreach part of this project is of high importance because a substantial gap in online consumer privacy education and outreach for teens, seniors, minority, and under-served populations such as disabled adults and financially-challenged consumers exists. This gap specifically includes members of this cy pres class, and has not been adequately addressed, as discussed below. This consumer education gap is one WPF has been concerned about for some years now. We see it as essential to tailor educational materials that are highly factual directly to groups of consumers to as to best comminicate.

This project also provides for much-needed direct consumer support to consumers who have need of privacy assistance related to online disclosure risks and consequences.

1. Project Goals and Description

This project will fund a multi-faceted national consumer online privacy educational campaign that closes the gaps with appropriate educational materials and effective delivery methods for the content. The first goal of the project will be crafting appropriate and focused educational materials, which will range from video to print to curricula to online tips and other items, and will be specifically designed for each segment of consumers we are working to reach. For example, materials focused for teens, seniors, financially vulnerable, victims of crime, and other vulnerable populations. The second goal of the project is to provide direct consumer support and education to class members, and to ensure outreach so as to be proactive in assisting consumers.

The vision is for an inclusive approach, with focused, consumer privacy-specific materials reaching new audiences online and off, and collaboration with teachers and senior and other community center directors to ensure vital, appropriate, specific, and helpful online privacy messaging reaches these class members. Our deep and long privacy expertise and consumer assistance expertise combined with our ability and knowledge of executing national educational campaigns is an invaluable and significant asset in this work.

This project directly targets the consumer education goals of the cy pres, with a focus on reaching all consumers, and in particular, vulnerable consumers, with critically important privacy education that is tailored to prevent harms, provide solutions and direct consumer support to assist consumers who have gotten into privacy challenges online and need assistance. This is a three-year project.

2. Project Deliverables

The deliverables for this project take the information and materials from the online privacy research conducted in Project One and tailor the information specifically for dissemination to consumers nationally, and in particular tailor the information for dissemination to vulnerable populations.

Deliverables for the second project include:

The deliverables for this project will be tailored for vulnerable populations.

- Direct consumer support for duration of grant (3 years): support for consumer queries about online privacy via email and phone.

- Direct consumer outreach. (workshops, free-to-consumer training sessions both online and off, and other direct to consumer outreach.)
- Robust consumer privacy education (based on cy pres research) materials tailored for:
  - Teens
  - Seniors
  - Financially vulnerable
  - Victims of crime
  - Individuals with medical or other challenges
  - Underserved populations
  - Spanish speakers
- Consumer materials to be published include: (Materials will be published online, and some materials will also be printed for delivery to consumers who require or strongly prefer print delivery. Digital materials will be mobile compatible. Materials will also be made into podcasts.)
  - Tipsheets and focused consumer guides
  - One-pagers
  - Wallet cards
- 8 instructional videos (tailored to audience)
- Training curriculum (One training curriculum)

3. Why This Project is Needed

We are sensitive to meeting the specific needs of this cy pres class. WPF receives many consumer phone calls directly related to online privacy needs and problems. Most of them are from people who are online, but who did not realize some of their actions online had the possibility of bringing them harm. This project would provide fund-

ing to facilitate reaching more consumers with better-targeted privacy information, and to support consumers who need direct assistance in the sometimes messy job of cleaning up the impacts of harmful disclosures, including unintended consequences of self-disclosed information. The deliverables for this project will be measurable, robust, and substantial, and we will be able to sustain an educational effort in order to allow for adequate penetration of the privacy messaging.

As discussed previously, the consumer privacy education gap is significant. Focused, online-privacy-specific materials sensitive to this cy pres class in vulnerable population categories are currently unavailable. General online safety materials exist for a few of the segments, but the educational materials specific to the actual problems and challenges experienced by the cy pres class members and the requirements for assisting them and informing them of specific risks of online disclosures do not yet exist. Second, the class members this part of the project is focused on are the least likely to be touched by the currently available general Internet safety education that is conducted primarily online, as this education is most typically directed through outreach and education directed toward individuals with pre-existing baseline sets of computer skills, computers, and online privacy knowledge.

4. Project Requirements

To complete this three-year project we have allocated $460,000 total for staffing and materials to create the content, test the content with class members, create a rollout and distribution plan, and then execute that plan with the content. This will be a three year project.

Specifically, we will need the following materials and staff as discussed below:

- **Consumer content writing, editing, posting, maintenance:** We will use WPF staff to research, write, test, and finalize the consumer guide. (Please see organizational information for biographical summaries of our executive director and other collaborating experts for the writing/testing portion of this project.)

  Personnel, Consumer content, writing, editing, posting, maintenance:

  - Research, writing, editing – (Staff)
  - Research assistant, editing, posting, maintenance (Staff)
  - Writing, editing (Staff)
  - Research – fact checking (Staff, with outsourced fact check for second pass.)
  - Video – (Staff)
  - Content testing (First pass, staff. Second pass, outsourced)
  - Spanish Translation (Outsourced)

- **Content distribution and consumer outreach and educational plan:** We will use WPF staff, consult with the advisory board, and consult with a contractor to ensure the consumer education component is a robust part of the distribution, rollout, and consumer outreach.

  Personnel, Content distribution and consumer outreach and educational plan:

  - Consumer education director: WPF's consumer education director will be responsible for rolling out and executing the outreach segment of this project, which will include online and offline components.

- Consumer education assistance and outreach: Staff
- Project Oversight: Executive Director
- We anticipate hiring a contractor to assist the education director in the rollout phase and to assist in coordinating workshops, free-to-consumer training sessions both online and off, and other direct to consumer outreach.
- Direct consumer support: We anticipate hiring one person to provide direct consumer support via phone and email.

- **Web designer**: We will work with John Emerson to create the web pages and the visual components of the materials. We will create a section of the web site to facilitate direct consumer support for the materials and topics related to this grant. (Please see organizational information for his bio.)

Other Project Components:

- **Digital and print brochures, one-pagers, and wallet cards**: We will create digital materials that can be repurposed across many mediums, including paper. All materials will be distributed online, and we will give people the ability to further print out the materials via our site. (This would function very similarly to the FTC's consumer education print outs; see <http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html>.)
- **Curriculum materials for trainers, community leaders, teachers and educators in key outreach environments**: a vital part of this project is creating and delivering tailored materials to individuals who can reach further into the community and continue

doing so. We will craft curriculum materials to assist with this.

- **Workshops in key cities to "train the trainers":** In order to complete a national rollout, we will hold three to four workshops that will bring together community workers serving the class members. We will provide training funded by this Cy Pres to give them the tools they need to provide direct assistance to class members. We have already completed a similar national rollout of this kind of program for medical identity theft, and national privacy training for National Network to End Domestic Violence trainers.

5. Budget for Project Two

The budget for Project Two is $475,000 over three years.

Expenses:

Personnel

Research (7-8 tailored consumer guides and other materials, curriculum) $50,000 (research focus will be on tailoring content appropriately for each segment. Research will include consulting with specialists and experts in each segment area for correct consumer approach for the segment, including content approach and materials and presentation approach.)

Writing (Including Spanish language materials): $50,000

Review and Fact Check: (Full review, including technical, and review by experts and testing for consumer comprehension.) $10,000

Translation (Consumer materials, including guides) Will be dependent on length, estimated $3,000

Video/Editing: (8 videos, including videos with Spanish translation) $20,000

Final proofing of electronic and print consumer education deliverables: $8,000

Web/consumer education materials layout (7-8 tailored consumer guides and additional listed materials, plus curriculum): $10,000

Consumer Education/ Outreach/ Training: $50,000 per year, x 3 years = $150,000

Consumer workshops (Personnel costs, 3-4 workshops): $15,000

Infographic design for data flows and illustrations (illustrations wiii be used in printed/digital materials for consumers and training curriculum and will be tailored to the audience.): $10,000

Direct consumer support/helpline: (dedicated personnel support for responding to consumer queries, provide consumer assistance) $35,000 per year x 3 = $105,000

Web site modifications to facilitate consumer support via online queries: $3,000

Other Project Expenses:

Costs directly associated with the proposed project.

Project Postage: $3,000 (We anticipate mailing more materials as part of the consumer outreach).

Project Printing: $5,000

Project Travel: $5,000

Web hosting costs directly associated with supporting the project: $3,000

Consumer Workshops (3-4): $25,000

C. Overall Project Budget Narrative (Both Projects)

We are allocating a budget of 1,020,000 over a period of 3 years to complete the two interrelated projects described in this grant. Project One is allocated $540,000 over three years, Project Two is allocated $475,000 over three years. The specific allocations are discussed under each project, above. We are budgeting $5,000 for unexpected costs. Any unused funding will be directed toward direct consumer support.

We are allocating the funds fully toward fulfilling the proposal deliverables, with zero general operations overhead or fringe benefits taken from the funds. Operational funds are directly related to project implementation only. As an organization focused solely on consumer privacy research and consumer privacy education, all grant funds will go toward the purpose of completing the proposed project that meets the needs of the cy pres settlement. WPF's mission and purpose is entirely privacy-focused.

An independent review board will be overseeing implementation of the grant, and ensure all grant funds are used for the purposes of the grant as specified in this proposal. WPF will be reporting grant disbursements throughout the project to the board for transparency purposes and to ensure strict adherence to the proposal budget. The review board members' biographical summaries are included in the addendum.

The projects are interrelated in that the research relevant to the cy pres class is created in Project One, and the general and targeted (vulnerable populations) national educational campaign and direct support and proactive consumer outreach and education are supported in Project Two.

Project Incidental Costs as part of operations and personnel:

We anticipate incidental costs directly related to this grant to accrue as we complete these projects. We are allocating a small portion of the grant to cover unexpected project-related costs such as printing deliverables, mailing deliverables, and other costs directly related to completing the grant. In a three-year grant, we do not expect the cost to be zero, neither do we expect it to be in excess of $5,000. We are budgeting $5,000 over a period of three years for this category. Any remainder monies will go toward direct consumer support.

D. Conflict of Interest Statement

The World Privacy Forum does not have any known conflicts with this cy pres.

Staff: No one on staff has worked for Google, and no one on staff has done a project for Google. No one on staff has family members who work for Google.

Board: No member of the board has worked for Google, and no one on the board has done a project for Google. No one on the board has family members who work for Google.

Operational control: WPF is an independent public interest research group. No one at Google, on staff or associated, has any operational control over WPF. No Google employees or directors, or former Google employees or directors have oversight over any WPF projects.

WPF Project oversight: WPF undertakes significant research and public education projects. Our projects are independent, and no one from Google has oversight of any WPF projects, or ever has. For this project, WPF has created an independent advisory board, none of

whom work for Google. The advisory board's biographical summaries are included in the addendum.

Funding: Our funding comes from foundation grants, cy pres, individual donations, and corporate donations. Our policy and practice is that all corporate funds, if and when accepted, are strictly for general support only, and there are no stipulations or strings attached. We strongly protect our independence, and we make this clear to all funders.

In the past three years specifically, our funding has come from foundation grants, cy pres, individual donations, and general support from commercial companies. We have accepted general support funding from Google with no strings attached. Prior and during the funding period, we have demonstrated complete independence from the funding, and have explicitly and effectively spoken out about Google privacy practices we deemed incorrect and have undertaken work to get those practices corrected. For example, in 2012 we submitted a complaint to the FTC about Google's Safari practices. That complaint is available on our website. The complaint was effective. In its settlement press release, the FTC specifically mentioned WPF. Over the years, we have been very active and effective in calling attention to practices that we question regarding Google. We wrote and disseminated a 31-group sign on letter in 2004 regarding Gmail practices. In 2010 we questioned some of the cloud practices the city of Los Angeles was seeking to put in place, particularly in regard to HIPAA among some other privacy concerns. At the time, this was a Google project. We have a reputation for fairness and firmness, and it is one we have worked hard for. When a company misbehaves and jeopardizes consumer privacy, we will and we do speak up.

E. Organizational Details and Contact Information

Pam Dixon, Executive Director, is the primary contact for the World Privacy Forum.

We are located at:

World Privacy Forum
3108 Fifth Avenue, Suite B
San Diego, CA 92103

The World Privacy Forum has current and active 501 C 3 status.

EIN number: 35-2241027

Part III. Addendum

This addendum includes more detailed information about the World Privacy Forum, our work, testimony, biographical summaries of independent project advisory board, WPF project staff, and WPF publications.

A. World Privacy Forum Organizational Background

1. About WPF

The World Privacy Forum[2] is a non-profit, nonpartisan 501(c)(3) public interest research and consumer education group focused on conducting in-depth research and consumer education in the area of privacy, with a focus on health care privacy and technology. Our core mission is to provide substantive research and consumer information that documents and analyzes critically important privacy issues and to provide consumer information and educational support in the area of privacy. We also provide direct support to consumers. Our work has often broken critical new ground, and the World Pri-

---

[2] <http://www.worldprivacyforum.org>.

vacy Forum's reports and consumer information have achieved extremely high visibility and credibility, as well as enjoying short and long-term positive impacts.

Our reports and work on Online Privacy, Data Brokers, Mobile privacy, Digital Signage, Medical ID Theft, Personal Health Records, HIPAA, Gentic privacy, and pharmacy and pharmacogenomic privacy have had substantial impact at a policy level, and at a consumer level. Our work in mobile privacy led to a national "nutrition label" standard privacy policy for mobile app developers in 2013. A California medical data breach notification bill was introduced as a result of a recommendation in our Medical ID theft report. That bill is now California law. Medical ID theft is a commonly known crime now; in 2006, we coined the term and documented this crime for the first time. We published the first report and consumer guide to warn about the privacy and confidentiality risks of PHRs, or Personal Health Records, especially those held outside of HIPAA protections. We published the first guide to HIPAA for patients, which is still the only guide of its kind. We have, for three years, cochaired the California Privacy and Security Advisory Board, a California state-level board that reports to the California Secretary of Health. We have been the consumer representative in the process of developing privacy and security guidelines for electronic health record exchanges in California. We have had substantive impacts in many other medical privacy areas, which we discuss in more detail below.

The World Privacy Forum is based in San Diego, California.

The World Privacy Forum fills a unique need for unbiased, in-depth public interest research with a focus on consumer privacy and education. Our work is almost en-

tirely focused on benefitting and educating consumers of all ages, and a good portion of our work is focused on California consumers. (Particularly in technology and health care privacy.)

The Forum was founded in 2003, and is incorporated and based in California. The Forum has achieved measurable and consistent success in each project it has undertaken, and receives consistent, very high-profile press coverage of its activities, as well as consistently high praise from regulators, legislators, academics, and consumers. The New York Times, Wall Street Journal, Time, BusinessWeek, Los Angeles Times, San Francisco Chronicle, NBC, CBS, ABC, and many others have covered World Privacy Forum activities and materials.

WPF has a combined total of 35 years of experience in general privacy policy, privacy analysis, research, legislation, writing, and documentation. We have long experience in researching, documenting, and educating consumers about new and existing areas of privacy inquiry.

A list of our publications may be found at http://www.worldprivacyforum.org/topics.html.

Some highlights include:

- *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* <http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/>
- *Data Brokers and the Federal Government: A New Front in the* Battle for Privacy Opens <http://www.worldprivacyforum.org/2013/10/report-data-brokers-and-the-federal-government-a-new-front-in-the-battle-for-privacy-opens/>.

- *Paying Out of Pocket to Protect Your Health Privacy: A New but Complicated HIPAA Option.* <http://www.worldprivacyforum.org/2014/01/wpf-report-paying-out-of-pocket-to-protect-health-privacy/>.
- *Medical ID Theft: The Information Crime that Can Kill You* <http://www.worldprivacyforum.org/medicalidentitytheft.html>.
- *A Patient's Guide to HIPAA* (updated with the Sept. 2013 changes to HIPAA.) http://www.worldprivacyforum.org/hipaa/index.html>.
- *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* <http://www.worldprivacyforum.org/cloudprivacy.html>.
- *Personal Health Records: Why Many PHRs Threaten Privacy* <http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf>.
- *PHR Consumer Guide* <http://www.worldprivacyforum.org/pdf/WPF_PHRConsumerAdvisory_02_20_2008fs.pdf>.
- *Genetic Privacy Page (Key issues, detailed comments, and resources.)* http://www.worldprivacyforum.org/geneticprivacy.html.
- *The Two Way Mirror Society: Privacy Implications of the New Digital Signage Networks* <http://www.worldprivacyforum.org/pdf/onwaymirrorsocietyfs.pdf>
- *Consumer principles for Digital Signage Networks, including child protection principles* <http://www.worldprivacyforum.org/pdf/DigitalSignageprinciplesfs.pdf>.

- *Consumer Guide to Medical ID Theft* <http://www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html>.
- *Top Ten Opt Outs* <http://www.worldprivacyforum.org/toptenoptout.html>.
- *Many regulatory filings on privacy, including filings on FTC PHR Data Breach regulations, the Genetic Information NonDiscrimination Act (GINA), many filings on HIPAA to HHS, and numerous filings on California health privacy regulations.*

2. WPF Online Privacy Projects

A key focus of WPF is online privacy. We work nationally, internationally, and at the state level. We note that we have conducted other work, for example biometric research, however we highlight this work in particular here due to its relevance to the cy pres class.

Online Privacy Reference Book: Bob Gellman and Pam Dixon co-authored a definitive reference book on online privacy to be used in academic institutions (ABC-CLIO, 2012). During the course of writing the book, the WPF authors had the opportunity to interview leading people in the field and explore where the gaps are in online privacy.

Internet Privacy Project: WPF has maintained an Internet privacy project since opening its doors. Our first report was on job search online, our second major report was on online credit reports, and many other consumer tips and materials at WPF focus on online privacy. We are well-known for our work on cloud privacy as well as search privacy and online advertising privacy issues. WPF is the originator of Do Not Track, Pam Dixon coined the term, wrote the first Do Not Track proposal

and submitted it to the FTC during public testimony. Now DNT is a national and global idea, and it is actively being discussed regarding implementation. At least one state law has been passed regarding DNT.

Electronic Health Record Privacy: The WPF has also done a great deal of work in the area of online health records. The WPF served on the California steering committee for the national HISPC project, and has testified before the National Committee on Vital and Health Statistics on the privacy, security, and confidentiality issues relating to a National Health Information Network, and what that might look like for consumers.

We have published a significant report on Personal Health Records, which are online health records. Ours was the first privacy report on this important topic. We also published consumer education materials to go along with this report.

Most recently, in California, we assisted in the privacy review of California state's proposed regulations for Health Information Exchanges. After our review for the state, we wrote sample comments and circulated them to assist the privacy and consumer community in writing recommendations for more stringent privacy protections.

Co-Chair California Privacy and Security Advisory Board (Consumer representative): The WPF was appointed by the California Secretary of Health to the position of co-chair of the CalPSAB, a state board dedicated to increasing the medical privacy and security of health records in an electronic environment. Our role is as a consumer representative.

As consumer representative, we introduced and achieved a Fair Information Practices-based model for California privacy regulations. We also fought very hard

to require patient consent before medical records were exchanged in HIE systems. We were successful in that very long fight. Recently, we have assisted with the creation of privacy guidelines for HIEs in the state of California.

Online Pharmacy records privacy: The WPF has filed a substantial complaint over pharmaceutical marketing privacy with the Federal Trade Commission. That complaint is currently being reviewed by the FTC.

We are very proud of our work in achieving a fair result with the online iPledge system. We testified before the FDA twice in regards to an egregious privacy situation regarding the iPledge RiskMAP. (http://www.worldprivacyforum.org/pdf/WPF_RiskMAP_FDA28June2007fs.pdf and http://www.worldprivacyforum.org/pdf/WPF_FDAiPledge_08012007fs.pdf) Due to our testimony and efforts, (See also http://www.worldprivacyforum.org/pdf/NCVHS_letterWPF08022007fsw.pdf) the FDA iPledge RiskMAP (a program designed to reduce risks to patients on Accutane) patients taking Accutane are no longer bound by a privacy policy that allows the direct marketing of their privacy information.

We have also been very active in Pharmacogenomic recommendations at the Secretary's Advisory Committee on Genetics, Health and Society. We have been the only privacy group to file detailed comments on this important process. Our main interest has been to highlight the presence of marketing of consumers' genetic information online, outside of HIPAA. See http://www.worldprivacyforum.org/pdf/WPF_SACGHS_comments12192007fs.pdf, http://www.worldprivacyforum.org/pdf/WPF_SACGHS_05232007fs.pdf, more at worldprivacyforum.org.

3. Current WPF Projects

Currently, the World Privacy Forum is completing the following projects:

- We are completing the third in a series of major national data broker reports, to be published June 2014. (Two reports are already published, October 2013, and April 2014.).
- We are in the process of a significant Big Data project regarding vulnerable populations, with a focus on economically vulnerable populations and other vulnerable populations. (2014-2016).
- We are in the midst of our second medical ID theft report (2014).
- We completed and published a significant online opt-out informational tool for consumers, it is the largest data broker opt-out list available online. (Published December, 2013).
- We have completed the creation of an online informational clearinghouse of HIEs for California patients. (Phase I completed July 2012, Phase II completed July 2013. New materials will be published June 2014.)
- We published a major update of our popular guide, Patients' Guide to HIPAA, with full updates for changes in HIPAA that became law September, 2013. (Update published Sept. 20, 2013).
- We have completed a major national project on short form privacy notice for mobile applications, where WPF was a lead drafter. (June 2013.)

4. Operations and Budget

The majority of funding the World Privacy Forum receives goes directly related to its programs, not to GNA. Our operating budget reflects this. For these proposed

projects, costs are related directly to the project activities and the final deliverables.

Our annual operating budget is at an artificially depressed level because we are operating on a shoestring in regards to salaries. The Cy Pres funds would allow us to have a proper capacity funding of approximately $350,000 to $400,000 per year over three years, and would greatly increase our ability to execute our mission and purpose as an organization focused on protecting consumer privacy. We already have a strong team. We would give our current team more hours while still keeping costs as low as possible. We would add one person to focus on direct consumer support.

C. Biographical Summaries

The following individuals will work on the proposed projects.

A. Cy Pres Independent Advisory Board Biographical Summaries

As part of the cy pres grant proposal process, the World Privacy Forum has formed an advisory board to assist with the implementation and oversight of the cy pres funds and activities for the projects we have proposed. The role of the advisory board is provide oversight and transparency for the funds administration, to ensure the robust implementation of the grant programs, and assistance with fine-tuning any implementation issues that arise during the process of completing the grant activities. The Executive Director of WPF will regularly report on grant progress, funds use, and activities to the board so as to provide a trusted oversight mechanism.

Each member of the board has significant experience with national grant projects, and each has demonstrated

exceptional professional judgment as well as deep privacy expertise. Each individual has confirmed their desire to be included in this advisory board to assist pro bono with this grant process, and are excited about the proposed projects, which they see as being of significant value.

1. **Priscilla Regan, PhD and Chair. Department of Public and International Affairs, George Mason University**

Dr. Regan is a Professor in the Department of Public and International Affairs at George Mason University. Prior to joining that faculty in 1989, she was a Senior Analyst in the Congressional Office of Technology Assessment (1984-1989) and an Assistant Professor of Politics and Government at the University of Puget Sound (1979-1984). From 2005 to 2007, she served as a Program Officer for the Science, Technology and Society Program at the National Science Foundation. Since the mid-1970s, Dr. Regan's primary research interests have focused on both the analysis of the social, policy, and legal implications of organizational use of new information and communications technologies, and also on the emergence and implementation of electronic government initiatives by federal agencies.

Dr. Regan has published over forty articles or book chapters, as well as Legislating Privacy: Technology, Social Values, and Public Policy (University of North Carolina Press, 1995). As a recognized researcher in this area, Dr. Regan has testified before Congress and participated in meetings held by the Department of Commerce, Federal Trade Commission, Social Security Administration, and Census Bureau. She has received grants from the National Science Foundation. She was a member of the National Academy of Sciences, Computer Science

and Telecommunications Board, Committee on Authentication Technologies and their Privacy Implications. Dr. Regan received her PhD in Government from Cornell University and her BA from Mount Holyoke College.

2. Nathan Good, PhD.

Dr. Nathan Good is Principal of Good Research and Affiliate Researcher for UC Berkeley's TRUST center. A fundamental goal of his work is helping companies create networked systems devices and services that are simple, secure and respectful of people's privacy. He is a co-author of the UC Berkeley web privacy census, and contributing author to books on privacy and the user experience of security systems. Prior to Good Research, Nathan was at PARC, Yahoo and HP research labs.

At Berkeley, he worked with TRUST and the Samuelson Law & Technology Clinic and was a member of the 2007 California Secretary of State Top-to-Bottom Review of Electronic Voting Systems. Nathan has published extensively on user experience studies, privacy, and security related topics and holds patents on software technology for multimedia systems and event analysis.

His research has been reported on in the Economist, New York Times, CNN and ABC and he has testified on his research before the House, Senate and FTC. Nathan's recent work on Privacy and Design was recognized for a best paper award at the Privacy Law Scholars Conference, and was featured in both IAPP and the Future of Privacy Forums top 6 Privacy Papers for Policy Makers. Nathan has a PhD in Information Science and a MS in Computer Science from the University of California at Berkeley and was a member of LifeLock's Fraud Advisory Board.

3. Linda Ackerman, Esq.

Linda Ackerman is an attorney who specializes in privacy. She is a Ponemon Institute Distinguished Fellow, and was a principle contributor to the development of the California Attorney General's guide to medical identity theft. She has also written a number privacy and security policies and data sharing agreements for health information exchanges, and she has served as Chief Privacy Officer of the Long Beach Network for Health.

Previously, she was a member of a key national advisory board, the Transportation Security Administration's Secure Flight Working Group. She was also a member of the board of directors of the California Regional Health Information Organization (CalRHIO) and the Real ID Privacy and Security Workgroup convened by the California Office of Privacy Protection. As the co-founder of a nonprofit organization focused on consumer privacy, Ms. Ackerman learned about nonprofit corporate governance and continues to act as an attorney/advisor in that subject area.

Ms. Ackerman received her undergraduate degree from Mt. Holyoke College. She is a graduate of St. Louis University Law School and has an MA in history from San Francisco State University.

B. WPF Staff and Project Team Bios

1. Pam Dixon, Executive Director

Pam Dixon will be the principal investigator researching and writing the research and educational content for the proposed Cy Pres distribution projects. She will also be responsible for overseeing the video content for the projects, and will be the person who coordinates the final deliverables for the projects.

Pam Dixon is the founder and executive director of the World Privacy Forum, a public interest research and consumer education group she founded November 2003. The forum is based in San Diego, California. An author and a researcher, Dixon is the author of nine books, hundreds of articles, and numerous major research studies in the area of privacy, including her pioneering report on medical identity theft (World Privacy Forum, May 2006) and digital signage privacy (2010). Her most recent book, Online Privacy, is coauthored by Bob Gellman and was published by ABC-CLIO in 2012. Her new book, the A to Z of privacy, is being published in 2014.

Dixon's privacy research has been impactful on a national and international scale. Her data broker research, co-authored with Robert Gellman, has been widely disseminated and has been quoted by the White House in its policy paper on Big Data and privacy. Her medical ID theft report has resulted in the crime of medical identity theft to be brought into public view and recognized officially as a new crime beginning in 2007 by the Department of Justice and the FTC. The report has also led to new consumer protection legislation (medical data breach law) in California and other states as well as at the federal level. Her report on Digital Signage Networks led to Congressional testimony as well as an FTC hearing on the issue, and the consumer privacy principles she crafted on the topic were largely adopted. Recently, she was one of the lead drafters for short form privacy notices for mobile apps for the NTIA Department of Commerce multistakeholder process.

Pam Dixon has served as the co-chair of the California Privacy Security and Advisory Board, a position she was appointed to by the California Secretary of Health. Other recent reports include *The Two Way Mirror Society:*

Privacy Implications of the New Digital Signage Networks and *Privacy in the Clouds: Privacy and Security Implications of Cloud Computing*, among others. Pam Dixon was one of the experts who created the materials for the well-known *Patient's Guide to HIPAA* at the World Privacy Forum. This consumer guide is the first consumer guide to HIPAA written, and has been very well-received.

Formerly a research fellow and principal investigator with the Privacy Foundation at Denver University's Sturm School of Law, Dixon worked with famed Internet security and privacy expert Richard M. Smith on Privacy Foundation Projects. During her tenure there, Dixon focused in particular on researching and writing about workplace and technology-related privacy issues in a series of ground-breaking reports and consumer education guides. She was the principal investigator and author of the first report to consider the privacy of online job search sites, something that at the time was not even thought of as an issue.

Dixon is the recipient of a Johns Hopkins University Fellowship for outstanding teaching. Dixon's work has been covered extensively by the media, including Time, the New York Times, the Washington Post, Good Morning America, the BBC, Newsweek, the Wall Street Journal, Fortune, Readers' Digest, the Los Angeles Times, Business Week, the Associated Press, 48 Hours, CBS, NBC, ABC, CNN, Fox, PBS, MSNBC, and NPR. She was an on-air technology contributor to TechTV's Money Machine for two years, and is currently a ClearChannel Radio commentator on technology, privacy, and security matters. She has been a ClearChannel commentator for more than 7 years. A complete bio is available for Pam

Dixon at http://www.worldprivacyforum.org/aboutus.html.

Books and Articles:

Most recently, Pam Dixon co-authored *Online Privacy*, a reference book on online privacy along with co-author Robert Gellman. The book was published in 2012 by ABC CLIO books. She is the author of seven prior books published by Random House, John Wiley & Sons, Petersons, others. She has also written hundreds of articles for newspapers, primarily the Orange County Register and The San Diego Union Tribune. Also, numerous articles for World Privacy Forum web site, particularly consumer tips, privacy tips, etc. For more, see www.worldprivacyforum.org and see <http://www.pamdixon.com/articles.htm> for a selection of articles dating back to 1998.

Lectures, Testimony, highlights only:

- **US Federal Trade Commission**: March 2014, Alternate Consumer Scoring Products, testimony.
- **US Senate, Congressional Testimony**: December 2013, Testimony of Pam Dixon, Senate Commerce Committee, *What Information do Data brokers Have on Consumers?* <http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf>.
- **Biometrics 2013**: Biometric privacy, October 2013.
- **US Federal Trade Commission**: May 2013, Senior Identity Theft, testimony.
- **Visiting Scholar**: Pacific Northwest College of Art, Portland. (Privacy in a Modern Era, April 2013)
- **US Federal Trade Commission/IAPP**: Privacy in Developing Countries, March 2013)

- **US Department of Commerce**, June 2012-July 2013, NTIA Multistakeholder process, lead drafter of mobile online short form privacy notice.
- **CES Leaders in Technology**, January 2013.
- **Churchill Club**: January 2013, Privacy Gaps.
- **United States Congress**, Testimony of Pam Dixon Executive Director, World Privacy Forum Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, *What's a Consumer to Do? Consumer Perceptions and Expectations of Privacy Online*, October 13, 2011 <http://www.worldprivacyforum.org/2011/-10/public-comments-testimony-whats-aconsumer-to-do-consumer-perceptions-and-expectations-of-privacy-online/>.
- **United States Congress**, Testimony of Pam Dixon, Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce. *The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information November* 2009 <http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf>.
- **Federal Trade Commission**, 2009-2010, Privacy Roundtable Hearings, three segments of testimony about online privacy.
- **Federal Trade Commission**, April 2008, testimony on medical identity theft, personal health records, and genetic privacy issues.
- **Secretary's Advisory Committee on Genetics, Health, and Society**, February 2008, Testimony on direct-to-consumer genetic testing and privacy issues.

- **University of San Diego, Guest Lecturer**, February 2008, graduate class on genetics, ethics, and privacy.
- **Federal Trade Commission**, November 2007, Testimony on behavioral advertising, submission of report and consensus document.
- **Joint FDA /AHRQ Public Meeting**, June 26, 2007, Rockville, Maryland. Testimony on marketing uses of patient information in Risk Minimization Action Plans (RiskMAPs). Written testimony available.
- California Health Information Association Statewide Conference: **June 13, 2007. Presentation on Medical Identity Theft, solutions for victims and healthcare providers.**
- National Academies of Science, Institute of Medicine, Board on Health Sciences Policy meeting: **June 6, 2007, Washington, D.C. Formal presentation on Privacy and Genome-Wide Association Studies: Issues and Solutions.**
- **California State Assembly Health Committee**: April 24, 2007, expert testimony on medical identity theft and data breach.
- **American Health Information Community (HHS)**: September 29, 2006, Washington DC. Testimony, *Medical Identity Theft and Authentication Issues.* Written testimony available.
- **The University of San Diego**: March 20, 2006. Panel discussion on China, the Internet, censorship, and privacy presented by KPBS, The Center for Ethics in Science & Technology and the Values Institute of the University of San Diego.
- **National Conference of State Legislatures Fall Forum**: Dec. 7, 2005, Chicago. Presentation on RFID and medical privacy in the hospital environment,

- **Neurosciences Institute, Center for Ethics in Science and Technology, San Diego:** "Searching the Internet: Who's Watching?" November 2, 2005,
- **National Committee on Vital and Health Statistics:** August 16, 2005, San Francisco, CA. Hearing of the Privacy and Confidentiality subcommittee. Testimony by Pam Dixon on medical privacy, medical records, electronic health records, and the proposed National Health Information Network.
- **California Senate Select Committee on the Legal, Social & Ethical Consequences of Emerging Technologies, Informational Hearing:** May 13 2005, San Diego. Expert testimony, Pam Dixon.

2. Robert Gellman, legal analysis, research, writing

Robert Gellman will be assisting in the writing and research for the projects. He will also conduct a fact review of the completed materials to ensure accuracy and fairness.

Robert Gellman is a privacy and information policy consultant in Washington, D.C. A graduate of the Yale Law School, Gellman has worked on information policy issues for more than 25 years. He worked for 17 years as chief counsel to a Subcommittee in the House of Representatives responsible for information policy activities, oversight, legislation, and reports on privacy matters, freedom of information, the Privacy Act of 1974, government information dissemination activities, health record confidentiality, archives, and other information policy matters. (Subcommittee on Information, Justice, Transportation, and Agriculture, House Committee on Government Operations.)

He served as a member of the Department of Health and Human Service's National Committee on Vital and Health Statistics (1996-2000), a federal advisory committee with responsibilities for health information infrastructure matters.

Mr. Gellman has worked with the World Privacy Forum on many of its key consumer reports and educational guides. His World Privacy Forum credits include the Medical Identity Theft report and guide, the Patient's Guide to HIPAA, Privacy in the Clouds (the first major privacy report on cloud computing to be published), and many others.

Publications: (Partial list only)

- *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010). Available here or here.
- *Why Deidentification Fails Research Subjects and Researchers*, 10 American Journal of Bioethics, 28-30 (2010). Available here.

  Health Privacy: The Way We Live Now, The Privacy Papers, Free Congress Foundation (2002 Second Quarter), available at <http://www.privacyrights.org/ar/gellman-med.htm>.
- *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 Hastings Law Journal 1183 (2003).
- *Twin Evils: Government Copyright and Copyright-Like Controls Over Government Information*, 45 Syracuse Law Review 999 (1995).
- *Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies*

of Privacy Costs are Biased and Incomplete (March 2002), available at <http://www.epic.org/reports/dmfprivacy.pdf> and at <http://www.cdt.org/publications/dmfprivacy.shtml>.

- *A General Survey of Video Surveillance Law in the United States* in Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy (2005) (T.M.C. Asser Press).
- *Designing Genetic Information Policy: The Need for an Independent Policy Review of the Ethical, Legal, and Social Implications of the Human Genome Project*, House Report 102-478 (1992).
- *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, VI Software Law Journal 199 (1993).
- *Public Records—Access, Privacy, and Public Policy: A Discussion Paper*, 12 Government Information Quarterly 391 (1995).

A complete list of Mr. Gellman's hundreds of publications is available at www.bobgellman.com.

3. Marianne Fitzpatrick, MBA

Marianne holds the position of Senior Project Manager. Her responsibilities include performing project management activities to ensure strategic objectives are achieved in a timely manner and accurately for the Forum. She is a compliance expert, and is deeply knowledgeable about consumer financial privacy. As such, she also participates in WPF projects, for example, the NTIA Multistakeholder process and the forthcoming WPF data broker research report.

Marianne is an MBA-degreed professional with extensive compliance managerial experience most recently at

JP Morgan Chase supporting the Bank's attorneys through Program Management activities such as:

- Chair, Weekly Operational Breaks Resolution Meetings with Legal, Senior Operations Managers, Audit and Compliance as well as other delegates from around the world.
- Led Semi Annual Unit Response to Corporate Audit and Compliance for Sarbanes Oxley (SOX). Change Management Unit Lead.
- Led Executive Complaints Resolution for items in a litigation status with the Bank, for example, Congressional, Office of Consumer Complaints.
- Policy and Procedure Subject Matter Expert (22 Unit Process Documentation Kits).
- Led Litigation projects such as Uniform Data Business Analytics, Washington Mutual Litigation Account conversion, Thin Client Conversion, Business Continuity Plan Development and more.

While at Chase, Marianne was selected as the 2009 Chase Portrait Honoree for outstanding demonstration of core values. She also received Multiple Top-Performer Awards and Honors and the Unit Scorecard was an Exceeds rating during her time at Chase.

4. Breann Robinson

Breann Robinson is Consumer Education Director, with special focus in the area of Teen, Senior, and vulnerable populations Privacy Awareness and Education. Breann has come on board WPF specifically to focus on creating consumer privacy education programs and to execute national roll-outs.

Breann's experience in consumer education programs was honed during her time as a Peace Corps Volunteer.

While in the Peace Corps, Breann worked with the Directorate of Public Health, in Albania (Burrel) where she designed and implemented successful school-based health campaigns. From initiating a Women's Health Campaign that was able to transport valuable health information and resources to six surrounding villages to developing a Dental Hygiene program that was taught to over 200 students, Breann made big strides to help her community. She also facilitated development and sustainability by providing English courses to students and Physicians, leading a weekly Book Club for women, and introducing an important SAT informational courses for youth.

Breann was also an Instructor at TERI, Inc. for developmentally disabled adults while she earned her Financial Management degree from California State University of Long Beach.

At the World Privacy Forum, Bree has been developing consumer privacy education programs and materials to target hard-to-reach consumers who have not been served by existing programs or materials. Her emphasis is on online privacy, and she is implementing the program in multiple mediums online and off.

5. Blake Hamilton, Media and Communications Fellow

Blake Hamilton is a photojournalist and investigative reporter. Blake has produced multiple video series for WPF, including a groundbreaking video series about Privacy in India shot on location in India, as well as a complete video consumer education kit for Health Information Exchanges, part of a grant project to create consumer education for this topic area. He has also crafted a series of biometric videos for WPF, a series which is ongoing. In addition to video, Blake assists with Spanish

language work at the WPF and serves as WPF's webmaster.

Blake's international portfolio includes environmental work, including filming, editing, and producing a short documentary on environmental challenges in the Chilean Salmon Farming Industry.

Other photography work includes contributions to Ethos Magazine, a student-run quarterly magazine, at the University of Oregon, where he also worked as a photo editor. In this position, Blake established an online version of the magazine. The website recently won the Columbia Scholastic Press Association's Collegiate Digital Magazine Silver Crown. Blake has lived in Argentina and Chile, is fluent in Spanish, and currently lives in San Diego, California.

6. John Emerson, data visualization text design

John Emerson is a highly regarded web and text designer and data visualization expert. He has crafted extensive web, text, ebook, and data visualization materials for WPF as well as the Committee to Project Journalists, UN Trust Fund to End Violence Against Women, Human Rights Watch, Amnesty International USA, Idealist.org, Center for Economic and Social Rights, Columbia University, and many others.

For the WPF, he has created the groundbreaking Medical ID theft map that visualizes 20 years of identity theft by zip code and city. He has also crafted WPF's HIE project map and other data visualizations and materials such as the Health Data Breach map.

His consultancy, Backspace, is a design consultancy dedicated to research, development and promotion of design in the public interest. See http://backspace.com/

is/in/the/house/work/web.html for more about his Backspace and John Emerson's work.